ESX 配置指南

ESX 4.1

vCenter Server 4.1

在本文档被更新的版本替代之前，本文档支持列出的每个产品的版本和所有后续版本。要查看本文档的更新版本，请访问 http://www.vmware.com/cn/support/pubs。

ZH_CN-000328-00



最新的技术文档可以从 VMware 网站下载：

http://www.vmware.com/cn/support/pubs/

VMware 网站还提供最近的产品更新信息。

您如果对本文档有任何意见或建议，请把反馈信息提交至：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

北京办公室
北京市海淀区科学院南路 2 号
融科资讯中心 C 座南 8 层
www.vmware.com/cn

上海办公室
上海市浦东新区浦东南路 999 号
新梅联合广场 23 楼
www.vmware.com/cn

广州办公室
广州市天河北路 233 号
中信广场 7401 室
www.vmware.com/cn

目录

网络

存储器

安全

主机配置文件

附录

关于本文档

本手册（《ESX 配置指南》）提供了有关如何为 VMware® ESX 配置网络的信息，其中包括如何创建虚拟交换机和端口，以及如何为虚拟机、VMware vMotion™ 和 IP 存储设置网络。此外还论述了如何配置文件系统及各种类型的存储器，如 iSCSI 和光纤通道。本指南提供了有关 ESX 中内置的安全功能的论述，以及为使 ESX 免遭攻击而可采取的措施。此外，它还包括一个 ESX 技术支持命令及其 VMware vSphere™ Client 等效指令的列表，以及 `vmkfstools` 实用程序的描述。

此信息涉及 ESX 4.1。

目标读者

本手册专为需要安装、升级或使用 ESX 的用户提供。本手册的目标读者为熟悉数据中心操作且具丰富经验的 Windows 或 Linux 系统管理员。

VMware 技术出版物词汇表

VMware 技术出版物提供了一个词汇表，其中包含一些您可能不熟悉的术语。有关 VMware 技术文档中所使用的术语的定义，请访问 http://www.vmware.com/support/pubs。

文档反馈

VMware 欢迎您提出宝贵建议，以便改进我们的文档。如有意见，请将反馈发送到 docfeedback@vmware.com。

VMware vSphere 文档

vSphere 文档包括 VMware vCenter Server 和 ESX 文档集。

图中使用的缩写

本手册中的图片使用表 1 中列出的缩写形式。

表 1 缩写

缩写	描述
数据库	vCenter Server 数据库
数据存储	受管主机的存储器
dsk#	受管主机的存储磁盘
hostn	vCenter Server 受管主机
SAN	受管主机之间共享的存储区域网络类型数据存储
tmplt	模板

表 1 缩写 （续）

缩写	描述
user#	具有访问权限的用户
VC	vCenter Server
VM#	受管主机上的虚拟机

技术支持和教育资源

您可以获取以下技术支持资源。有关本文档和其他文档的最新版本，请访问：
http://www.vmware.com/support/pubs。

在线支持和电话支持

要通过在线支持提交技术支持请求、查看产品和合同信息以及注册您的产品，请访问 http://www.vmware.com/support。

客户只要拥有相应的支持合同，就可以通过电话支持，尽快获得对优先级高的问题的答复。请访问 http://www.vmware.com/support/phone_support.html。

支持服务项目

要了解 VMware 支持服务项目如何帮助您满足业务需求，请访问
http://www.vmware.com/support/services。

VMware 专业服务

VMware 教育服务课程提供了大量实践操作环境、案例研究示例，以及用作作业参考工具的课程材料。这些课程可以通过现场指导、教室授课的方式学习，也可以通过在线直播的方式学习。关于现场试点项目及实施的最佳实践，VMware 咨询服务可提供多种服务，协助您评估、计划、构建和管理虚拟环境。要了解有关教育课程、认证计划和咨询服务的信息，请访问
http://www.vmware.com/services。

ESX 配置简介 1

本指南将介绍配置 ESX 主机网络、存储器和安全需要完成的任务。此外，本指南还提供有关有助于了解这些任务以及如何根据需要部署主机的概述、建议和概念性论述。

在使用此信息之前，请阅读《vSphere 简介》以了解系统结构以及组成 vSphere 系统的物理和虚拟设备的概述。

此简介概括了本指南的内容。

网络

网络信息使您了解物理和虚拟网络概念，介绍配置 ESX 主机的网络连接需要完成的基本任务，并对高级网络主题和任务进行论述。

存储器

存储器信息提供有关存储器的基本认识，介绍配置和管理 ESX 主机存储器所要执行的基本任务，并对如何设置裸设备映射 (RDM) 进行论述。

安全

安全信息介绍 VMware 已内置到 ESX 中的安全措施，以及为保护主机免受安全危胁所采取的措施。这些措施包括使用防火墙、利用虚拟交换机的安全功能以及设置用户身份验证和权限。

主机配置文件

本节介绍主机配置文件的功能，以及如何使用它将主机配置封装到主机配置文件。本节还将介绍如何将此主机配置文件应用于其他主机或群集、如何编辑配置文件以及如何检查主机是否与配置文件相符。

附录

附录提供有助于您配置 ESX 主机的专业信息。

- ESX 技术支持命令 - 论述了可通过命令行 Shell（如 Secure Shell (SSH)）发出的 ESX 配置命令。尽管有这些命令可供使用，但不要将其视为可在其上生成脚本的 API。这些命令可能有所更改，并且 VMware 不支持依赖于 ESX 配置命令的应用程序和脚本。此附录提供了对应于这些命令的 vSphere Client 等效指令。
- 使用 vmkfstools - 讨论 vmkfstools 实用程序，该程序可用于创建和操作主机上的虚拟磁盘、文件系统、逻辑卷和物理存储设备。

网络

网络简介 2

将讨论 ESX 网络的基本概念以及如何在 vSphere 环境中设置和配置网络。

本章讨论了以下主题：

网络概念概述

一些概念对透彻了解虚拟网络至关重要。如果您是 ESX 的新用户，则了解这些概念将对您很有帮助。

物理网络是为了使物理机之间能够收发数据而在物理机间建立的网络。VMware ESX 运行于物理机之上。

虚拟网络是运行于单台物理机之上的虚拟机之间为了互相发送和接收数据而相互逻辑连接所形成的网络。虚拟机可连接到在添加网络时创建的虚拟网络。

物理以太网交换机管理物理网络上计算机之间的网络流量。一台交换机可具有多个端口，每个端口都可与网络上的一台计算机或其他交换机连接。可按某种方式对每个端口的行为进行配置，具体取决于其所连接的计算机的需求。交换机将会了解到连接其端口的主机，并使用该信息向正确的物理机转发流量。交换机是物理网络的核心。可将多个交换机连接在一起，以形成较大的网络。

虚拟交换机 vSwitch 的运行方式与物理以太网交换机十分相似。它检测与其虚拟端口进行逻辑连接的虚拟机，并使用该信息向正确的虚拟机转发流量。可通过使用物理以太网适配器（也称为上行链路适配器）将虚拟网络连接至物理网络，以将 vSwitch 连接到物理交换机。此类型的连接类似于将物理交换机连接在一起以创建较大型的网络。即使 vSwitch 的运行方式与物理交换机十分相似，但它不具备物理交换机所拥有的一些高级功能。

vNetwork 分布式交换机在数据中心上的所有关联主机之间充当单一 vSwitch。这使得虚拟机可在跨多个主机进行迁移时确保其网络配置保持一致。

dvPort 是 vNetwork 分布式交换机上的一个端口，连接到主机的服务控制台或 VMkernel，或者连接到虚拟机的网络适配器。

端口组为每个端口指定了诸如宽带限制和 VLAN 标记策略之类的端口配置选项。网络服务通过端口组连接 vSwitch。端口组定义通过 vSwitch 连接网络的方式。通常，单个 vSwitch 与一个或多个端口组关联。

dvPort 组是与 vNetwork 分布式交换机关联的端口组，它为每个成员端口指定端口配置选项。dvPort 组定义如何通过 vNetwork 分布式交换机连接到网络。

当多个上行链路适配器与单一 vSwitch 相关联以形成小组时，就会发生网卡绑定。小组将物理网络和虚拟网络之间的流量负载分摊给其所有或部分成员，或在出现硬件故障或网络中断时提供被动故障切换。

VLAN 可用于将单个物理 LAN 分段进一步分段，以便使端口组中的端口互相隔离，就如同位于不同物理分段上一样。标准是 802.1Q。

VMkernel TCP/IP 网络堆栈支持 iSCSI、NFS 和 vMotion。虚拟机运行其自身系统的 TCP/IP 堆栈，并通过虚拟交换机连接至以太网级别的 VMkernel。

IP 存储器是指将 TCP/IP 网络通信用作其基础的任何形式的存储器。iSCSI 可用作虚拟机数据存储，NFS 可用作虚拟机数据存储并用于直接挂载 .ISO 文件，这些文件对于虚拟机显示为 CD-ROM。

TCP 分段卸载 (TSO) 可使 TCP/IP 堆栈发出非常大的帧（达到 64 KB），即使接口的最大传输单元 (MTU) 较小也是如此。然后网络适配器将较大的帧分成 MTU 大小的帧，并预置一份初始 TCP/IP 标头的调整后副本。

借助“通过 vMotion 迁移”，可将已启动的虚拟机从一台 ESX 主机转移到另一台，而无需关闭虚拟机。可选 vMotion 功能需要其自身的许可证密钥。

网络服务

vNetwork 向主机和虚拟机提供了多种不同服务。

可以在 ESX 中启用三种类型的网络服务：

- 将虚拟机连接到物理网络以及相互连接虚拟机。
- 将 VMkernel 服务（如 NFS、iSCSI 或 vMotion）连接至物理网络。
- 通过服务控制台运行 ESX 管理服务。服务控制台端口（默认情况下在安装期间设置）是将 ESX 连接至任何网络或远程服务（包括 vSphere Client）所必需的。其他服务（如 iSCSI 存储器）可能需要其他服务控制台端口。

在 vSphere Client 中查看网络信息

vSphere Client 显示了一般网络信息及网络适配器的特定信息。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 （可选）选择要查看的网络类型。

选项	描述
虚拟交换机	显示主机上的 vNetwork 标准交换机网络。
vNetwork 分布式交换机	显示主机上的 vNetwork 分布式交换机网络。

vNetwork 分布式交换机选项仅出现在与一个或多个 vNetwork 分布式交换机连接的主机上。

即会显示主机上的每个虚拟交换机的网络信息。

在 vSphere Client 中查看网络适配器信息

您可以查看主机上的每个物理网络适配器的有关信息，如速度、双工和观察的 IP 范围。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 单击**配置**选项卡，然后单击**网络适配器**。

网络适配器面板显示了以下信息。

表 2–1 网络适配器参数

选项	描述
设备	网络适配器的名称。
速度	网络适配器的实际速度和双工。
已配置	网络适配器的已配置速度和双工。
交换机	网络适配器相关联的 vSwitch 或 vDS。
观察的 IP 范围	网络适配器可访问的 IP 地址。
支持 LAN 唤醒	网络适配器支持 LAN 唤醒功能。

vNetwork 标准交换机的基本网络 3

vNetwork 标准交换机 (vSwitches) 处理 vSphere 环境中主机级别的网络流量。

使用 vSphere Client，添加基于以下类别的网络，这些类别反映网络服务类型：

- 虚拟机
- VMkernel
- 服务控制台

本章讨论了以下主题：

vNetwork 标准交换机

可以创建名为 vNetwork 标准交换机 (vSwitch) 的抽象网络设备。vSwitch 可在虚拟机之间进行内部流量路由或链接至外部网络。

使用 vSwitch 组合多个网络适配器的带宽并平衡它们之间的通信流量。也可将 vSwitch 配置为处理物理网卡故障切换。

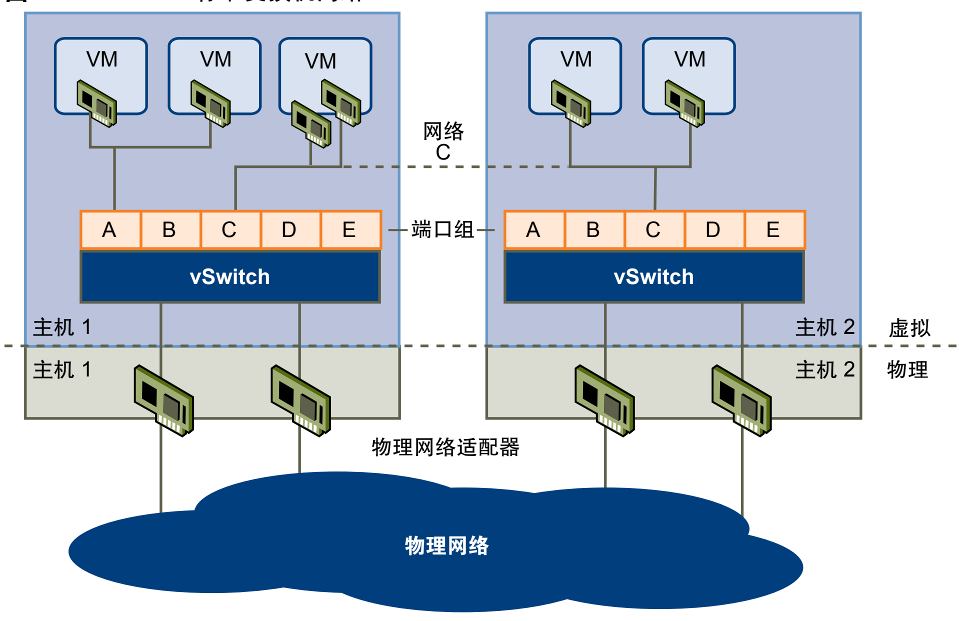
vSwitch 模拟物理以太网交换机。vSwitch 的默认逻辑端口数量为 120。可以每个端口连接虚拟机的一个网络适配器。与 vSwitch 关联的每个上行链路适配器均使用一个端口。vSwitch 的每个逻辑端口都是单一端口组的成员。还可向每个 vSwitch 分配一个或多个端口组。有关允许的最大端口和端口组数的信息，请参见《vSphere 4.1 的最大配置》。

当两个或多个虚拟机连接到同一 vSwitch 时，它们之间的网络流量就会在本地进行路由。如果将上行链路适配器连接到 vSwitch，每个虚拟机均可访问该适配器所连接到的外部网络。

端口组

端口组将多个端口聚合在一个公共配置下，并为连接到带标记网络的虚拟机提供稳定的定位点。

图 3–1 vNetwork 标准交换机网络



每个端口组都由一个对于当前主机保持唯一的网络标签来标识。使用网络标签，可以使虚拟机配置可在主机间移植。对于数据中心中物理连接到同一网络的所有端口组（即每组都可以接收其他组的广播），会赋予同一标签。反过来，如果两个端口组无法接收对方的广播，则会赋予不同的标签。

VLAN ID 是可选的，它用于将端口组流量限制在物理网络内的一个逻辑以太网网段中。要使端口组到达其他 VLAN 上的端口组，必须将 VLAN ID 设置为 4095。如果使用 VLAN ID，则必须一起更改端口组标签和 VLAN ID，以便标签能够正确地表示连接性。

虚拟机的端口组配置

可以从 vSphere Client 添加或修改虚拟机端口组。

vSphere Client 的添加网络向导将引导您完成与虚拟机相连的虚拟网络的创建任务，该任务包括创建 vSwitch 和配置网络标签设置。

设置虚拟机网络时，需要考虑是否在主机之间的网络中迁移虚拟机。如果需要，请确保两台主机均位于同一广播域（即同一第 2 层子网）内。

ESX 不支持在不同广播域中的主机之间进行虚拟机迁移，因为迁移后的虚拟机可能需要在其被移至另一个网络后不再可访问的系统和资源。即使网络配置设置为高可用性环境或包括可解决不同网络中虚拟机需求的智能交换机，当 ARP 表格为虚拟机进行更新并恢复网络流量时，仍会遇到网络延迟。

虚拟机通过上行链路适配器接入物理网络。只有当一个或多个网络适配器连接到 vSwitch 时，vSwitch 才能将数据传输到外部网络。当两个或多个适配器连接到单个 vSwitch 时，它们便以透明方式进行组合。

添加虚拟机端口组

虚拟机端口组为虚拟机提供网络连接。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 选择“虚拟交换机”视图。

vSwitch 将显示在包括详细信息布局的概述中。

4 在页面右侧，单击**添加网络**。

5 接受默认连接类型（**虚拟机**），然后单击**下一步**。

6 选择**创建虚拟交换机**或所列出的一台现有 vSwitch 及其关联物理适配器，以用于此端口组。

创建新的 vSwitch 不一定要使用以太网适配器。

如果创建的 vSwitch 不带物理网络适配器，则该 vSwitch 上的所有流量仅限于其内部。物理网络上的其他主机或其他 vSwitch 上的虚拟机均无法通过此 vSwitch 发送或接收流量。如果想要一组虚拟机互相进行通信但不与其他主机或虚拟机组之外的虚拟机进行通信，则可创建一个不带物理网络适配器的 vSwitch。

7 单击**下一步**。

8 在“端口组属性”组中，输入用于标识所创建的端口组的网络标签。

网络标签用于标识两个或多个主机共有且与迁移兼容的连接。

9 （可选）如果使用的是 VLAN，在 **VLAN ID** 字段中输入一个介于 1 和 4094 之间的数字。如果使用的不是 VLAN，则将此处留空。

如果输入 0 或将该选项留空，则端口组只能看到未标记的（非 VLAN）流量。如果输入 4095，端口组可检测到任何 VLAN 上的流量，而 VLAN 标记仍保持原样。

10 单击**下一步**。

11 确定 vSwitch 配置正确之后，单击**完成**。

VMkernel 网络配置

VMkernel 网络接口用于 VMware vMotion、IP 存储器和容错。

在主机之间移动虚拟机称为迁移。使用 vMotion，可以在不停机的情况下迁移已启动的虚拟机。必须正确设置 VMkernel 网络连接堆栈，以容纳 vMotion。

IP 存储器是指将 TCP/IP 网络通信用作其基础的任何形式的存储器，包括用于 ESX 的 iSCSI、FCoE 和 NFS。由于这些存储器类型都基于网络，因此它们可使用相同的 VMkernel 接口和端口组。

VMkernel 提供的网络服务（iSCSI、NFS 和 vMotion）使用 VMkernel 中的 TCP/IP 堆栈。此 TCP/IP 堆栈与用于服务控制台中的 TCP/IP 堆栈完全隔离。其中的每个 TCP/IP 堆栈均通过连接到一个或多个 vSwitch 上的一个或多个端口组来访问各种网络。

VMkernel 级别的 TCP/IP 堆栈

VMware VMkernel TCP/IP 网络堆栈以多种方式为它所处理的各种服务提供网络支持。

VMkernel TCP/IP 堆栈用以下方式处理 iSCSI、NFS 和 vMotion。

- 作为虚拟机数据存储的 iSCSI。
- 用于直接挂载 `.ISO` 文件的 iSCSI，.ISO 文件对于虚拟机显示为 CD-ROM。

- 作为虚拟机数据存储的 NFS。
- 用于直接挂载 `.ISO` 文件的 NFS，.ISO 文件对于虚拟机显示为 CD-ROM。
- 通过 vMotion 迁移。
- 容错日志记录。
- 为从属硬件 iSCSI 适配器提供网络信息。

如果有两个或更多的物理网卡用于 iSCSI，则可以通过配置 iSCSI 多路径创建软件 iSCSI 的多个路径。有关 iSCSI 多路径的详细信息，请参见《iSCSI SAN 配置指南》。

注意 ESX 仅支持 TCP/IP 上的 NFS 版本 3。

设置 VMkernel 网络

创建用作 vMotion 接口或 IP 存储器端口组的 VMkernel 网络适配器。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 在“虚拟交换机”视图中，单击**添加网络**。

4 选择 **VMkernel**，然后单击**下一步**。

5 选择要使用的 vSwitch，或选择**创建虚拟交换机**以创建一个新的 vSwitch。

6 选中与 vSwitch 要使用的网络适配器相对应的复选框。

为每个 vSwitch 选择适配器，以便使通过适配器连接的虚拟机或其他设备可访问正确的以太网分段。如果“创建新的虚拟交换机”下方未出现适配器，则表明系统中的所有网络适配器均被现有 vSwitch 使用。可以在不使用网络适配器的情况下创建新的 vSwitch，也可以选择由现有 vSwitch 使用的网络适配器。

7 单击**下一步**。

8 选择或输入网络标签和 VLAN ID。

选项	描述
网络标签	用于识别所创建端口组的名称。此标签是在配置诸如 VMkernel 服务（如 vMotion 和 IP 存储器）的过程中，配置要连接到此端口组的虚拟适配器时指定的。
VLAN ID	用于识别端口组网络流量将使用的 VLAN。

9 选择**将此端口组用于 vMotion**，以便允许此端口组对另一个主机将其自身通告为应在其中发送 vMotion 流量的网络连接。

对于每个主机来说，只能为其中一个 vMotion 和 IP 存储器端口组启用此属性。如果没有为任何端口组启用此属性，则无法通过 vMotion 向此主机进行迁移。

10 选择是否将此端口组用于容错日志记录。

11 在启用了 IPv6 的主机上，选择是否使用 **IP (默认值)**、**IPv6** 或 **IP 和 IPv6 网络**。

在没有启用 IPv6 的主机上，此选项不会显示。IPv6 配置不能与从属硬件 iSCSI 适配器配合使用。

12 单击**下一步**。

13 选择**自动获得 IP 设置**以使用 DHCP 获得 IP 设置，或选择**使用以下 IP 设置**来手动指定 IP 设置。

如果选择手动指定 IP 设置，则提供此信息。

DHCP 不能与从属硬件 iSCSI 适配器配合使用。

a 输入 VMkernel 接口的 IP 地址和子网掩码。

此地址必须不同于为服务控制台设置的 IP 地址。

b 单击**编辑**以设置 VMkernel 服务（如 vMotion、NAS 和 iSCSI）的 VMkernel 默认网关。

c 默认情况下，**DNS 配置**选项卡上已输入主机名称。

如同域一样，在安装期间指定的 DNS 服务器地址也已预先选定。

d 在**路由**选项卡中，服务控制台和 VMkernel 均需要其自身的网关信息。

如果要连接到与服务控制台或 VMkernel 不在同一个 IP 子网上的计算机，则需要网关。默认设置为静态 IP 设置。

e 单击**确定**，然后单击**下一步**。

14 如果要针对 VMkernel 接口使用 IPv6，请选择以下选项之一来获取 IPv6 地址。

- **通过 DHCP 自动获取 IPv6 地址**
- **通过路由器通告自动获取 IPv6 地址**
- **静态 IPv6 地址**

15 如果选择使用静态 IPv6 地址，请完成以下步骤。

a 单击**添加**以添加新的 IPv6 地址。

b 输入 IPv6 地址和子网前缀长度，然后单击**确定**。

c 要更改 VMkernel 默认网关，请单击**编辑**。

16 单击**下一步**。

17 检查信息，单击**上一步**以更改条目，然后单击**完成**。

服务控制台配置

服务控制台和 VMkernel 均使用虚拟以太网适配器连接至 vSwitch 并到达 vSwitch 所服务的网络。

常见服务控制台配置修改包括更改网卡和为使用中的网卡更改设置。

如果仅有一个服务控制台连接，则不允许更改服务控制台配置。对于新连接，请将网络设置更改为使用其他网卡。在确保新连接运行正常之后，请移除旧连接。这会切换至新网卡。

在 ESX 中最多可创建 16 个服务控制台端口。

设置服务控制台网络

单个服务控制台网络接口是在 ESX 安装过程中设置的。在 ESX 正常运行之后，还可以添加其他服务控制台接口。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 在“虚拟交换机”视图中，单击**添加网络**。

4 选择**服务控制台**，然后单击**下一步**。

5 选择要用于网络访问的 vSwitch，或选择**创建新的 vSwitch**，然后单击**下一步**。

   如果“创建虚拟交换机”组中未出现适配器，则表明系统中的所有网络适配器均被现有 vSwitch 使用。

6 输入网络标签和 VLAN ID，然后单击**下一步**。

7 输入 IP 地址和子网掩码，或选择**自动获得 IP 设置**。

8 单击**编辑**以设置服务控制台默认网关，然后单击**下一步**。

9 在启用了 IPV6 的主机上，选择**不使用 IPv6 设置**以便针对服务控制台仅使用 IPv4 设置，或选择**使用以下 IPv6 设置**为服务控制台配置 IPv6。

   如果在主机上禁用了 IPv6，此屏幕不会出现。

10 如果选择使用 IPv6，请选择如何获得 IPv6 地址。

11 如果选择**静态 IPv6 地址**，则执行以下操作：

   a 单击**添加**以添加新的 IPv6 地址。

   b 输入 IPv6 地址和子网前缀长度，然后单击**确定**。

   c 要更改服务控制台默认网关，请单击**编辑**。

12 单击**下一步**。

13 检查信息，单击**上一步**以更改条目，然后单击**完成**。

配置服务控制台端口

可以编辑服务控制台端口属性，例如 IP 设置和网络连接策略。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 在页面右侧，单击要编辑的 vSwitch 的**属性**。

4 在“vSwitch 属性”对话框中，单击**端口**选项卡。

5 选择**服务控制台**，然后单击**编辑**。

6 要继续配置服务控制台，请单击**继续修改此连接**。

7 根据需要编辑端口属性、IP 设置和有效策略。

8 单击**确定**。

设置默认网关

可以为服务控制台的每个 TCP/IP 堆栈配置一个默认网关。路由不适用于软件 iSCSI 多路径配置或从属硬件 iSCSI 适配器。



小心 保存更改之前，请确保网络设置正确。如果网络设置的配置有误，UI 会丢失与主机的连接，随后您必须从服务控制台的命令行重新对主机进行配置。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和 **DNS 和路由**。

3 单击**属性**。

4 单击**路由**选项卡。

5 在“服务控制台”下方，设置服务控制台网络的默认网关和网关设备。

对于服务控制台，仅当两个或多个网络适配器使用同一子网时才需要网关设备。网关设备确定用于默认路由的网络适配器。

服务控制台和VMkernel通常连接到不同的网络，因此需要其各自的网关信息。连接的计算机与服务控制台或VMkernel 接口位于不同 IP 子网上时需要网关。

在启用了 IPv6 的主机上，还可以选择服务控制台网络的“IPv6 的默认网关”和“使用 IPv6 的网关设备”。

6 在“VMkernel”下方，设置 VMkernel 网络的默认网关。

在启用了 IPv6 的主机上，还可以选择 VMkernel 网络的“IPv6 的默认网关”。

7 单击**确定**。

显示服务控制台信息

可以查看服务控制台网络信息，如 VLAN ID 和网络策略。

步骤

1 单击服务控制台端口组左侧的信息图标以显示服务控制台信息。

2 单击 **X**，以关闭信息弹出窗口。

对服务控制台使用 DHCP

大多数情况下，应对服务控制台使用静态IP 地址。如果DNS 服务器可将服务控制台的主机名称映射至动态生成的 IP 地址，也可将服务控制台设置为使用动态地址 DHCP。

如果DNS 服务器无法将主机名称映射至其DHCP 生成的IP 地址，则使用服务控制台的数值IP 地址访问主机。当 DHCP 租期到期或系统重新引导时，数值 IP 地址可能会发生变化。因此，VMware 建议不要将 DHCP 用于服务控制台，除非 DNS 服务器可处理主机名称转换。

vNetwork 标准交换机属性

vNetwork 标准交换机设置可控制端口的 vSwitch 层面默认值，而每个 vSwitch 的端口组设置均可覆盖这些值。您可以编辑 vSwitch 属性，如上行链路配置和可用端口数。

更改 vSwitch 的端口数

vSwitch 可用作使用了一组常用网络适配器的端口配置（包括根本不包含网络适配器的集合）的容器。每个虚拟交换机都提供有限数量的端口，虚拟机和网络服务可以通过这些端口访问一个或多个网络。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 在页面右侧，单击要编辑的 vSwitch 的**属性**。

4 单击**端口**选项卡。

5 在“配置”列表中选择 vSwitch 项目，然后单击**编辑**。

6 单击**常规**选项卡。

7 从下拉菜单中选择您要使用的端口数。

8 单击**确定**。

下一步

重新启动系统后更改才会生效。

更改上行链路适配器的速度

可以更改上行链路适配器的连接速度和双工。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 选择 vSwitch 并单击**属性**。

4 单击**网络适配器**选项卡。

5 要更改网络适配器的已配置速度和双工值，请选择网络适配器并单击**编辑**。

6 要手动选择连接速度，请在下拉菜单中选择速度和双工。

   如果网卡和物理交换机在协商正确的连接速度时可能失败，请手动选择连接速度。速度和双工不匹配的表现包括低带宽，或者没有链路连接。

   适配器以及与它所连接到的物理交换机端口必须设置为相同值，如两者可同时设置为“auto”或“ND”（其中 ND 表示某个速度和双工），但不能一个设置为“auto”，另一个设置为“ND”。

7 单击**确定**。

添加上行链路适配器

可以将多个适配器与一个 vSwitch 关联以提供成网卡绑定。此网卡组可以共享流量并提供故障切换。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 选择 vSwitch 并单击**属性**。

4 单击**网络适配器**选项卡。

5 单击**添加**以启动添加适配器向导。

6 在列表中选择一个或多个适配器，然后单击**下一步**。

7 （可选）要将网卡重新排序到不同类别中，请选择网卡，并单击**上移**和**下移**。

选项	描述
活动适配器	vSwitch 使用的适配器。
备用适配器	如果一个或多个活动适配器发生故障，则备用适配器将成为活动适配器。

8 单击**下一步**。

9 查看“适配器摘要”页面上的信息，单击**上一步**以更改条目，然后单击**完成**。

   此时将重新出现网络适配器列表，显示现在由 vSwitch 声明的适配器。

10 单击**关闭**，退出“vSwitch 属性”对话框。

   在**配置**选项卡的“网络”区域中按指定的顺序和类别显示网络适配器。

Cisco 发现协议

Cisco 发现协议 (CDP) 允许 ESX 管理员决定哪个 Cisco 交换机端口与给定的 vSwitch 相连。当特定 vSwitch 启用了 CDP 时，可以通过 vSphere Client 查看 Cisco 交换机的属性（如设备 ID、软件版本和超时）。

在 ESX 主机上启用 CDP

默认情况下，vSwitch 设置为检测 Cisco 端口信息。还可以设置 CDP 模式，以便 Cisco 交换机管理员可以使用 vSwitch 信息。

步骤

1 直接登录 ESX 主机的控制台。

2 通过输入 **esxcfg-vswitch -b <vSwitch>** 命令查看 vSwitch 的当前 CDP 模式。

  如果禁用了 CDP，则模式将显示为**关闭**。

3 通过输入 **esxcfg-vswitch -B <mode> <vSwitch>** 命令更改 CDP 模式。

模式	描述
关闭	CDP 处于禁用状态。
侦听	ESX 检测并显示与关联 Cisco 交换机端口相关的信息，但并不向 Cisco 交换机管理员提供有关 vSwitch 的信息。
播发	ESX 将有关 vSwitch 的信息提供给 Cisco 交换机管理员，但不检测和显示 Cisco 交换机的相关信息。
二者	ESX 检测并显示与关联 Cisco 交换机相关的信息，并将有关 vSwitch 的信息提供给 Cisco 交换机管理员。

在 vSphere Client 上查看 Cisco 交换机信息

当 CDP 设置为**侦听**或**二者**时，可以查看 Cisco 交换机信息。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 单击 vSwitch 右侧的信息图标。

注意 由于 CDP 通常每分钟播发一次 Cisco 设备信息，因此从启用 ESX 的 CDP 到从 vSphere Client 获得 CDP 数据间可能会有显著的延迟。

vNetwork 分布式交换机的基本网络 4

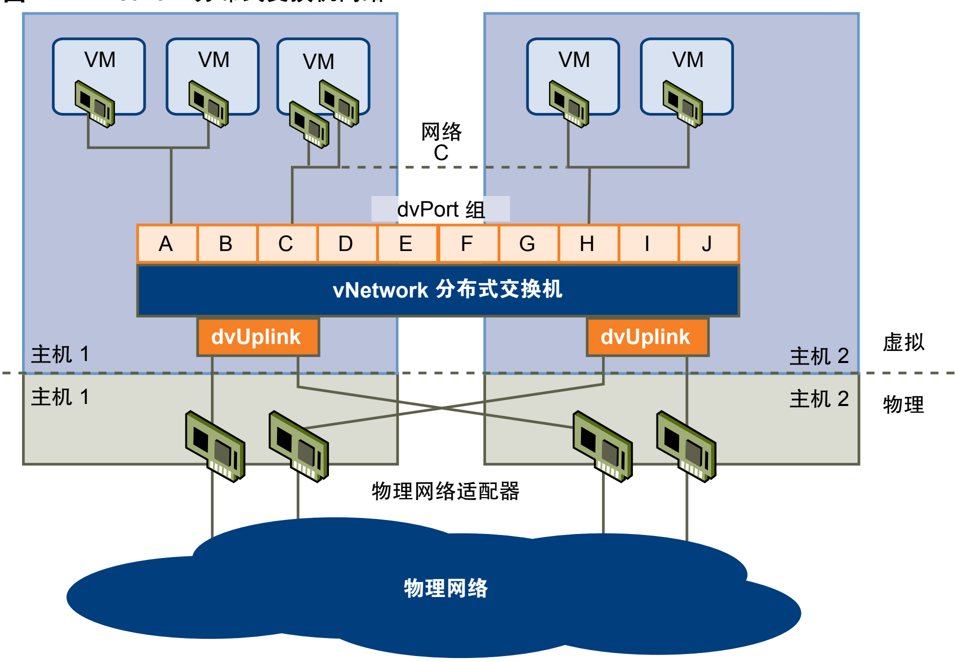
这些主题指导您掌握 vNetwork 分布式交换机网络的基本概念，并指导您如何在 vSphere 环境中设置和配置 vNetwork 分布式交换机网络。

本章讨论了以下主题：

vNetwork 分布式交换机架构

vNetwork 分布式交换机 (vDS) 在所有关联主机之间作为单个虚拟交换机使用。这使您能够设置跨所有成员主机的网络配置，并使得虚拟机可在跨多个主机进行迁移时保持其网络配置一致。

图 4–1 vNetwork 分布式交换机网络



与 vNetwork 标准交换机一样，每个 vNetwork 分布式交换机也是虚拟机可以使用的网络集线器。vNetwork 分布式交换机可在虚拟机之间转发内部流量，或者通过连接物理以太网适配器（也称为上行链路适配器）链接至外部网络。

您还可以为每个 vNetwork 分布式交换机分配一个或多个 dvPort 组。dvPort 组将多个端口组合在一个通用配置下，并为连接标定网络的虚拟机提供稳定的定位点。每个 dvPort 端口组都由一个对于当前数据中心唯一的网络标签来标识。VLAN ID 是可选的，它用于将端口组流量限制在物理网络内的一个逻辑以太网网段中。

利用网络资源池，可以按网络流量的类型来管理网络流量。

除了 VMware vNetwork 分布式交换机以外，vSphere 4 还为第三方虚拟交换机提供支持。有关配置这些第三方交换机的信息，请转至 http://www.cisco.com/go/1000vdocs。

配置 vNetwork 分布式交换机

可以在 vCenter Server 数据中心上创建 vNetwork 分布式交换机。创建了 vNetwork 分布式交换机之后，便可以添加主机、创建 dvPort 组并编辑 vNetwork 分布式交换机的属性和策略。

创建 vNetwork 分布式交换机

创建 vNetwork 分布式交换机以处理数据中心上相关主机的网络流量。

步骤

1 登录到 vSphere Client 并选择“网络”清单视图。

2 从“清单”菜单，选择**数据中心 > 新建 vNetwork 分布式交换机**。

3 选择 vNetwork 分布式交换机版本。

选项	描述
vNetwork 分布式交换机版本：4.0	与 ESX 版本 4.0 及更高版本兼容。不支持与更高版本 vDS 一起发布的功能。
vNetwork 分布式交换机版本：4.1.0	与 ESX 版本 4.1 及更高版本兼容。

4 单击**下一步**。

5 在“名称”文本框中输入 vNetwork 分布式交换机的名称。

6 使用箭头按扭选择 **dvUplink 端口数**，然后单击**下一步**。

dvUplink 端口将 vNetwork 分布式交换机连接到关联主机上的物理网卡。dvUplink 端口数是允许每台主机与 vNetwork 分布式交换机建立的最大物理连接数。

7 选择将主机添加到 vDS 的时间。

选项	描述
立即添加	通过单击每个主机或适配器旁边的复选框来选择要使用的主机和物理适配器。在 vNetwork 分布式交换机创建期间，只能添加尚未使用的物理适配器。
以后添加	此时不将主机添加到 vDS。必须在添加网络适配器之前将主机添加到 vDS。可以使用管理主机功能从 vSphere Client 的主机配置页面添加网络适配器，也可以使用主机配置文件进行添加。

8 单击**下一步**。

9 （可选）选择**自动创建默认端口组**。

此选项将创建一个带有 128 个端口的静态绑定端口组。对于具有复杂端口组要求的系统，跳过默认端口组并在完成 vNetwork 分布式交换机的添加之后创建新 dvPort 组。

10 查看 vNetwork 分布式交换机关系图以确保正确配置，然后单击**完成**。

将主机添加到 vNetwork 分布式交换机

创建 vDS 之后，可以在 vDS 级别将主机和物理适配器添加到 vNetwork 分布式交换机。

步骤

1 在 vSphere Client 中，选择“网络”清单视图，然后选择 vNetwork 分布式交换机。

2 选择**清单 > vNetwork 分布式交换机 > 添加主机**。

3 选择要添加的主机。

4 在所选主机下面，选择要添加的物理适配器，然后单击**下一步**。

可以选择可用的和使用中的物理适配器。

注意 将物理适配器移动到 vDS 而没有移动任何关联虚拟适配器可能导致这些虚拟适配器失去网络连接。

5 对于每个虚拟适配器，请从下拉菜单中选择**目标端口组**以将虚拟适配器迁移到 vDS，或者选择**不迁移**。

6 单击**下一步**。

7 （可选）将虚拟机网络迁移到 vDS。

a 选择**迁移虚拟机网络**。

b 对于每个虚拟机，请从下拉菜单中选择**目标端口组**，或者选择**不迁移**。

8 单击**下一步**。

9 检查 vDS 的设置，然后单击**完成**。

如果需要进行任何更改，请单击**上一步**以回到适当屏幕。

管理 vDS 上的主机

将主机和物理适配器添加到 vDS 后，可以在 vDS 上更改其配置。

步骤

1 在 vSphere Client 中，选择“网络”清单视图，然后选择 vNetwork 分布式交换机。

2 选择**清单 > vNetwork 分布式交换机 > 管理主机**。

3 选择要管理的主机，然后单击**下一步**。

4 选择要添加的物理适配器，取消选中要移除的物理适配器，然后单击**下一步**。

5 对于每个虚拟适配器，请从下拉菜单中选择**目标端口组**以将虚拟适配器迁移到 vDS，或者选择**不迁移**。

6 单击**下一步**。

7 （可选）将虚拟机网络迁移到 vDS。

a 选择**迁移虚拟机网络**。

b 对于每个虚拟机，请从下拉菜单中选择**目标端口组**，或者选择**不迁移**。

8 单击**下一步**。

9 检查 vDS 的设置，然后单击**完成**。

如果需要进行任何更改，请单击**上一步**以回到适当屏幕。

编辑常规 vNetwork 分布式交换机设置

可以编辑 vNetwork 分布式交换机的常规属性，例如 vNetwork 分布式交换机名称和 vNetwork 分布式交换机的上行链路端口数。

步骤

1 在 vSphere Client 中，选择“网络”清单视图，并选择 vNetwork 分布式交换机。

2 从“清单”菜单中，选择 **vNetwork 分布式交换机 > 编辑设置**。

3 选择**常规**以编辑下面的 vNetwork 分布式交换机设置。

- 输入 vNetwork 分布式交换机的名称。
- 选择上行链路端口数。
- 要编辑上行链路端口名称，请单击**编辑 dvUplink 端口名称**，输入新名称，然后单击**确定**。
- 输入任何有关 vNetwork 分布式交换机的备注。

4 单击**确定**。

编辑 vNetwork 分布式交换机高级设置

使用“vNetwork 分布式交换机设置”对话框可以配置高级 vNetwork 分布式交换机设置（如 vNetwork 分布式交换机的 Cisco 发现协议和最大 MTU）。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 vNetwork 分布式交换机。

2 从“清单”菜单中，选择 **vNetwork 分布式交换机 > 编辑设置**。

3 选择**高级**以编辑下面的 vNetwork 分布式交换机属性。

   a 指定最大 MTU 大小。

   b 选中**启用 Cisco 发现协议**复选框以启用 CDP，然后将操作设置为**侦听**、**通告**或**二者**。

   c 在“管理员联系信息”区域中输入 vNetwork 分布式交换机管理员的名称和其他详细信息。

4 单击**确定**。

查看 vNetwork 分布式交换机的网络适配器信息

从 vSphere Client 的网络清单视图中，查看 vNetwork 分布式交换机的物理网络适配器和上行链路分配。

步骤

1 在 vSphere Client 中，选择“网络”清单视图，并选择 vNetwork 分布式交换机。

2 从“清单”菜单中，选择 **vNetwork 分布式交换机 > 编辑设置**。

3 在**网络适配器**选项卡上，可以查看关联主机的网络适配器和上行链路分配。

   此选项卡是只读的。vNetwork 分布式交换机网络适配器必须在主机级别上进行配置。

4 单击**确定**。

将 vDS 升级到更新版本

可以将 vNetwork 分布式交换机版本 4.0 升级到版本 4.1，这使 vDS 能够利用仅在较高版本中可用的功能。

步骤

1 在 vSphere Client 中，选择“网络”清单视图，然后选择 vNetwork 分布式交换机。

2 在**摘要**选项卡上，在**版本**旁边，选择**升级**。

   升级向导详细介绍了对已升级的 vDS 可用的功能，早期版本中不提供这些功能。

3 单击**下一步**。

   升级向导列出了与此 vDS 关联的主机，而不管它们是否与已升级的 vDS 版本兼容。仅当所有主机都与新 vDS 版本兼容时，才能继续升级。

   升级向导将在每个不兼容的主机旁边列出不兼容的原因。

4 单击**下一步**。

5 验证列出的升级信息是否正确，然后单击**完成**。

dvPort 组

dvPort 组为 vNetwork 分布式交换机上的每个端口指定端口配置选项。dvPort 组定义如何连接到网络。

添加 dvPort 组

可使用创建 dvPort 组向导将 dvPort 组添加到 vNetwork 分布式交换机。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 vNetwork 分布式交换机。

2 从**清单**菜单中，选择**分布式虚拟交换机 > 新建端口组**。

3 输入 dvPort 组的名称和端口数。

4 选择 VLAN 类型。

选项	描述
无	不使用 VLAN。
VLAN	在 **VLAN ID** 字段中，输入一个介于 1 和 4094 之间的数字。
VLAN 中继	输入 VLAN 中继范围。
专用 VLAN	选择专用 VLAN 条目。如果尚未创建任何专用 VLAN，则此菜单为空。

5 单击**下一步**。

6 单击**完成**。

编辑 dvPort 组常规属性

使用 dvPort 组属性对话框可以配置 dvPort 组常规属性（如 dvPort 组名称和端口组类型）。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 dvPort 组。

2 从“清单”菜单中，选择**网络 > 编辑设置**。

3 选择**常规**以编辑以下 dvPort 组属性。

选项	操作
名称	输入 dvPort 组的名称。
描述	输入 dvPort 组的简要描述。
端口数	输入 dvPort 组的端口数。
端口绑定	选择将端口分配到与该 dvPort 组相连的虚拟机的时间。 ■ 虚拟机连接到 dvPort 组后，请选择**静态绑定**以将端口分配到虚拟机。 ■ 连接到 dvPort 组之后首次启动虚拟机时，请选择**动态绑定**以将端口分配到虚拟机。 ■ 为无端口绑定选择**极短**。只有当直接连接到 ESX 主机时，才可以选择极短绑定。

4 单击**确定**。

编辑 dvPort 组高级属性

使用“dvPort 组属性”对话框可以配置 dvPort 组高级属性（如端口替代设置）。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 dvPort 组。

2 从“清单”菜单中，选择**网络 > 编辑设置**。

3 选择**高级**以编辑 dvPort 组属性。

   a 选择**允许替代端口策略**以允许替代每个端口上的 dvPort 组策略。

   b 单击**编辑替代设置**以选择可以替代哪些策略。

   c 选择是否允许实时移动端口。

   d 选择**断开连接时配置重置**以在从虚拟机断开 dvPort 时放弃每个端口的配置。

4 单击**确定**。

dvPort

dvPort 是 vNetwork 分布式交换机上的一个端口，用于连接主机的服务控制台或 VMkernel，或者虚拟机的网络适配器。

默认 dvPort 配置是由 dvPort 组设置确定的，但可以在每个 dvPort 上替代各个 dvPort 的某些设置。

监控 dvPort 状况

vSphere 可以监控 dvPort 并提供关于每个 dvPort 的当前状态的信息。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 vNetwork 分布式交换机。

2 在**端口**选项卡上，单击**开始监控端口状态**。

此时在 vNetwork 分布式交换机的**端口**选项卡上的**状态**列中，将显示每个 dvPort 的当前状态。

表 4–1 dvPort 状态

状态	描述
已连接	此 dvPort 的链接已打开。
已断开	此 dvPort 的链接已关闭。
已阻止	此 dvPort 已阻止。
--	当前此 dvPort 的状态不可用。

配置 dvPort 设置

使用“端口设置”对话框可以配置常规 dvPort 属性（如端口名称和描述）。

步骤

1 登录到 vSphere Client，此时会显示 vNetwork 分布式交换机。

2 在**端口**选项卡上，右键单击要修改的端口，然后选择**编辑设置**。

3 单击**常规**。

4 修改端口名称和描述。

5 单击**确定**。

专用 VLAN

专用 VLAN 用于解决某些网络设置的 VLAN ID 限制和 IP 地址浪费。

专用 VLAN 由其主专用 VLAN ID 标识。主专用 VLAN ID 可以拥有多个与其关联的次专用 VLAN ID。主专用 VLAN 为**杂乱模式**，以便专用 VLAN 上的端口可以与配置为主专用 VLAN 的端口通信。次专用 VLAN 上的端口可以是**已隔离**（仅与杂乱模式端口通信），也可以是**团体**（与同一次专用 VLAN 上的杂乱模式端口和其他端口通信）。

如果要在 ESX 主机和其余物理网络之间使用专用 VLAN，则与 ESX 主机相连的物理交换机必须支持专用 VLAN，而且需要用 ESX 所用的 VLAN ID 进行配置以获取专用 VLAN 功能。对于使用基于动态 MAC+VLAN ID 进行学习的物理交换机，必须首先将所有相应的专用 VLAN ID 输入到交换机的 VLAN 数据库中。

要配置 dvPorts 以使用专用 VLAN 功能，必须在与 dvPorts 连接的 vNetwork 分布式交换机上创建必要的专用 VLAN。

创建专用 VLAN

可以创建专用 VLAN 以便在 vNetwork 分布式交换机及其关联的 dvPort 上使用。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 vNetwork 分布式交换机。

2 从**清单**菜单中，选择 **vNetwork 分布式交换机 > 编辑设置**。

3 选择**专用 VLAN** 选项卡。

4 在“主专用 VLAN ID”下面，单击**[在此输入专用 VLAN ID]**，并输入主专用 VLAN 号。

5 在对话框中的任何位置单击，然后选择刚才添加的主专用 VLAN。

添加的主专用 VLAN 将出现在“次专用 VLAN ID”下面。

6 对于每个新的次专用 VLAN，请单击“次专用 VLAN ID”下的**[在此输入专用 VLAN ID]**，然后输入次专用 VLAN 号。

7 在对话框中的任何位置单击，选择刚才添加的次专用 VLAN，然后选择**已隔离**或**团体**端口类型。

8 单击**确定**。

移除主专用 VLAN

从 vSphere Client 的网络清单视图中移除未使用的主专用 VLAN。

前提条件

在移除专用 VLAN 之前，确保没有配置任何端口组使用它。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 vNetwork 分布式交换机。

2 从**清单**菜单中，选择 **vNetwork 分布式交换机 > 编辑设置**。

3 选择**专用 VLAN** 选项卡。

4 选择要移除的主专用 VLAN。

5 在“主专用 VLAN ID”下单击**移除**，然后单击**确定**。

  移除主专用 VLAN 还将移除所有关联的次专用 VLAN。

移除次专用 VLAN

从 vSphere Client 的网络清单视图中移除未使用的次专用 VLAN。

前提条件

在移除专用 VLAN 之前，确保没有配置任何端口组使用它。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 vNetwork 分布式交换机。

2 从**清单**菜单中，选择 **vNetwork 分布式交换机 > 编辑设置**。

3 选择**专用 VLAN** 选项卡。

4 选择主专用 VLAN 以显示其关联的次专用 VLAN。

5 选择要移除的次专用 VLAN。

6 在“次专用 VLAN ID”下单击**移除**，然后单击**确定**。

配置 vNetwork 分布式交换机网络适配器

主机配置页面的“vNetwork 分布式交换机”网络视图显示主机的关联 vNetwork 分布式交换机的配置，并允许配置 vNetwork 分布式交换机网络适配器和上行链路端口。

管理物理适配器

对于具有关联 vNetwork 分布式交换机的每台主机，必须对 vNetwork 分布式交换机分配物理网络适配器或上行链路。每台主机上仅可为 vNetwork 分布式交换机上的每个上行链路端口分配一个上行链路。

将上行链路添加到 vNetwork 分布式交换机

对于具有关联 vNetwork 分布式交换机的每台主机，必须至少对 vNetwork 分布式交换机分配一个物理网络适配器或上行链路。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

  此时将出现所选主机的硬件配置页面。

2 依次单击**配置**选项卡和**网络**。

3 选择 **vNetwork 分布式交换机**视图。

4 单击**管理物理适配器**。

5 对于要向其添加上行链路的上行链路端口，请单击**单击以添加网卡**。

6 选择要添加的物理适配器。

  如果选择已连接到其他交换机的适配器，它将从该交换机中移除并重新分配给此 vNetwork 分布式交换机。

7 单击**确定**。

从 vNetwork 分布式交换机中移除上行链路

可以从 vNetwork 分布式交换机中移除上行链路或物理网络适配器。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

  此时将显示该服务器的硬件配置页面。

2 依次单击**配置**选项卡和**网络**。

3 选择 **vNetwork 分布式交换机**视图。

4 单击**管理物理适配器**。

5 单击**移除**，从 **vNetwork 分布式交换机**中移除上行链路。

6 单击**确定**。

管理虚拟网络适配器

虚拟网络适配器通过 vNetwork 分布式交换机处理主机网络服务。

可以通过关联的 vNetwork 分布式交换机（即通过创建新虚拟适配器或迁移现有虚拟适配器），为 ESX 主机配置服务控制台和 VMkernel 虚拟适配器。

在 vNetwork 分布式交换机上创建 VMkernel 网络适配器

创建用作 vMotion 接口或 IP 存储器端口组的 VMkernel 网络适配器。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 选择“vNetwork 分布式交换机”视图。

4 单击**管理虚拟适配器**。

5 单击**添加**。

6 选择**新建虚拟适配器**，然后单击**下一步**。

7 选择 **VMkernel**，然后单击**下一步**。

8 为虚拟适配器选择 dvPort 或 dvPort 组连接。

选项	描述
选择端口组	从下拉菜单中为要连接至的虚拟适配器选择 dvPort 组。
选择端口	从下拉菜单中为要连接至的虚拟适配器选择 dvPort。

9 选择**将此虚拟适配器用于 vMotion** 以便将此端口组作为发送 vMotion 流量的网络连接向另一个 ESX 主机报告。

  只能为每台 ESX 主机的一个 vMotion 和 IP 存储器端口组启用此属性。如果没有为任何端口组启用此属性，则无法通过 vMotion 向此主机进行迁移。

10 选择是否**将此虚拟适配器用于容错日志记录**。

11 在“IP 设置”下，指定 IP 地址和子网掩码。

  IPv6 不能与从属硬件 iSCSI 适配器配合使用。

12 单击**编辑**以设置 VMkernel 服务（如 vMotion、NAS 和 iSCSI）的 VMkernel 默认网关。

13 默认情况下，**DNS 配置**选项卡上已输入主机名称。在安装期间指定的 DNS 服务器地址和域也预先选定。

14 在**路由**选项卡中，服务控制台和 VMkernel 均需要其自身的网关信息。如果要连接到与服务控制台或 VMkernel 不在同一个 IP 子网上的计算机，则需要网关。

    静态 IP 设置为默认值。不要将路由与软件 iSCSI 多路径配置或从属硬件 iSCSI 适配器配合使用。

15 单击**确定**，然后单击**下一步**。

16 单击**完成**。

在 vNetwork 分布式交换机上创建服务控制台网络适配器

可以在 vNetwork 分布式交换机上创建服务控制台网络适配器，以便处理 vDS 上主机的服务控制台网络。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 选择“vNetwork 分布式交换机”视图。

4 单击**管理虚拟适配器**。

5 单击**添加**。

6 选择**新建虚拟适配器**，然后单击**下一步**。

7 选择**服务控制台**，然后单击**下一步**。

8 为虚拟适配器选择 dvPort 或 dvPort 组连接。

选项	描述
选择端口组	从下拉菜单中为要连接至的虚拟适配器选择 dvPort 组。
选择端口	从下拉菜单中为要连接至的虚拟适配器选择 dvPort。

9 输入 IP 地址和子网掩码，或选择**自动获得 IP 设置**。

10 （可选）单击**编辑**，设置服务控制台默认网关。

11 单击**下一步**。

12 单击**完成**。

将现有的虚拟适配器迁移到 vNetwork 分布式交换机

可以将 vNetwork 标准交换机上的现有虚拟适配器迁移到 vNetwork 分布式交换机。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 选择“vNetwork 分布式交换机”视图。

4 单击**管理虚拟适配器**。

5 单击**添加**。

6 选择**迁移现有虚拟网络适配器**，然后单击**下一步**。

7 选择一个或多个要迁移的虚拟网络适配器。

8 对于每个选定的适配器，从**选择端口组**下拉菜单中选择一个端口组。

9 单击**下一步**。

10 单击**完成**。

将虚拟适配器迁移到 vNetwork 标准交换机

可以使用迁移到虚拟交换机向导将现有虚拟适配器从 vNetwork 分布式交换机迁移到 vNetwork 标准交换机。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

   此时将显示该服务器的硬件配置页面。

2 依次单击**配置**选项卡和**网络**。

3 选择 **vNetwork 分布式交换机**视图。

4 单击**管理虚拟适配器**。

5 选择要迁移的虚拟适配器，然后单击**迁移到虚拟交换机**。

   此时将显示迁移虚拟适配器向导。

6 选择适配器要迁移到的 vSwitch，然后单击**下一步**。

7 输入虚拟适配器的**网络标签**和 **VLAN ID**（可选），然后单击**下一步**。

8 单击**完成**迁移虚拟适配器并完成向导。

在 vNetwork 分布式交换机上编辑 VMkernel 配置

可以从关联主机编辑 vNetwork 分布式交换机上现有 VMkernel 适配器的属性。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 选择“vNetwork 分布式交换机”视图。

4 单击**管理虚拟适配器**。

5 选择要修改的 VMkernel 适配器，然后单击**编辑**。

6 为虚拟适配器选择 dvPort 或 dvPort 组连接。

选项	描述
选择端口组	从下拉菜单中为要连接至的虚拟适配器选择 dvPort 组。
选择端口	从下拉菜单中为要连接至的虚拟适配器选择 dvPort。

7 选择**将此虚拟适配器用于 vMotion** 以便将此端口组作为发送 vMotion 流量的网络连接向另一个 ESX 主机报告。

   只能为每台 ESX 主机的一个 vMotion 和 IP 存储器端口组启用此属性。如果没有为任何端口组启用此属性，则无法通过 vMotion 向此主机进行迁移。

8 选择是否**将此虚拟适配器用于容错日志记录**。

9 在“IP 设置”下，指定 IP 地址和子网掩码，或选择**自动获得 IP 设置**。

10 单击**编辑**以设置 VMkernel 服务（如 vMotion、NAS 和 iSCSI）的 VMkernel 默认网关。

11 单击**确定**。

在 vNetwork 分布式交换机上编辑服务控制台配置

可以在 vNetwork 分布式交换机上编辑现有服务控制台适配器的端口和 IP 设置。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。
2 依次单击**配置**选项卡和**网络**。
3 选择“vNetwork 分布式交换机”视图。
4 单击**管理虚拟适配器**。
5 选择要修改的服务控制台适配器，然后单击**编辑**。
6 为虚拟适配器选择 dvPort 或 dvPort 组连接。

选项	描述
选择端口组	从下拉菜单中为要连接至的虚拟适配器选择 dvPort 组。
选择端口	从下拉菜单中为要连接至的虚拟适配器选择 dvPort。

7 输入 IP 地址和子网掩码，或选择**自动获得 IP 设置**。
8 （可选）单击**编辑**，设置服务控制台默认网关。
9 单击**确定**。

移除虚拟适配器

从“管理虚拟适配器”对话框中的 vNetwork 分布式交换机中移除虚拟网络适配器。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。
2 依次单击**配置**选项卡和**网络**。
3 选择 **vNetwork 分布式交换机**视图。
4 单击**管理虚拟适配器**。
5 选择要移除的虚拟适配器，然后单击**移除**。

   此时会显示一个对话框，其中显示消息“您确定要移除 *<适配器名称>* 吗？”
6 单击**是**。

在 vNetwork 分布式交换机上配置虚拟机网络

可以通过配置单个虚拟机网卡，或通过从 vNetwork 分布式交换机自身迁移多组虚拟机，将虚拟机连接到 vNetwork 分布式交换机。

通过将虚拟机的关联虚拟网络适配器连接到 dvPort 组，可以将虚拟机连接到 vNetwork 分布式交换机。对于单个虚拟机，可以通过修改虚拟机的网络适配器配置来完成；对于虚拟机组，可以通过将虚拟机从现有虚拟网络迁移到 vNetwork 分布式交换机来完成。

将虚拟机迁入或迁出 vNetwork 分布式交换机

除了在单个虚拟机级别将虚拟机连接到 vNetwork 分布式交换机以外，还可以在 vNetwork 分布式交换机网络和 vNetwork 标准交换机网络之间迁移一组虚拟机。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 vNetwork 分布式交换机。

2 从**清单**菜单中，选择 **vNetwork 分布式交换机 > 迁移虚拟机网络**。

此时将显示迁移虚拟机网络向导。

3 在**选择源网络**下拉菜单中，选择要从中进行迁移的虚拟网络。

4 从**选择目标网络**下拉菜单中，选择要迁移到的虚拟网络。

5 单击**显示虚拟机**。

与要从中进行迁移的虚拟网络相关联的虚拟机即会在**选择虚拟机**字段中显示。

6 选择要迁移到目标虚拟网络的虚拟机，然后单击**确定**。

将单个虚拟机连接到 dvPort 组

通过修改虚拟机的网卡配置，将单个虚拟机连接到 vNetwork 分布式交换机。

步骤

1 登录 vSphere Client，在“清单”面板中选择虚拟机。

2 在**摘要**选项卡中，单击**编辑设置**。

3 在**硬件**选项卡上，选择虚拟网络适配器。

4 从**网络标签**下拉菜单中，选择要迁移到的 dvPort 组，然后单击**确定**。

网络 I/O 控制

网络资源池决定在 vDS 上为不同网络流量类型赋予的优先级。

当启用网络 I/O 控制时，vDS 流量划分为以下几种网络资源池：容错流量、iSCSI 流量、vMotion 流量、管理流量、NFS 流量和虚拟机流量。通过设置每个网络资源池的**物理适配器份额**和**主机限制**，可以控制这些网络资源池的流量的优先级。

分配给某个网络资源池的**物理适配器份额**确定提供给与该网络资源池关联的流量的总可用带宽份额。对某个网络资源池可用的传输带宽份额是由网络资源池的份额以及哪些其他网络资源池正在主动传输来确定的。例如，如果将容错流量和 iSCSI 流量资源池设置为 100 个份额，而将其他各资源池设置为 50 个份额，则容错流量和 iSCSI 流量资源池将各收到 25% 的可用带宽。其余资源池将各收到 12.5% 的可用带宽。仅当物理适配器饱和时才能应用这些预留。

注意 iSCSI 流量资源池份额不适用于从属硬件 iSCSI 适配器的 iSCSI 流量。

网络资源池的**主机限制**是网络资源池可以使用的带宽的上限。

启用 vDS 上的网络 I/O 控制

启用网络资源管理以使用网络资源池，从而按类型区分网络流量优先级。

前提条件

确认数据中心至少有一个 vNetwork 分布式交换机 4.1 版本。

步骤

1 在 vSphere Client 中，选择“网络”清单视图，然后选择 vNetwork 分布式交换机。

2 在**资源分配**选项卡上，单击**属性**。

3 选择**在此 vDS 上启用网络 I/O 控制**，然后单击**确定**。

编辑网络资源池设置

可以为每个网络资源池更改网络资源池设置，如资源池的已分配份额和限制。

步骤

1 在 vSphere Client 中，选择“网络”清单视图，然后选择 vNetwork 分布式交换机。

2 在**资源分配**选项卡上，右键单击要编辑的网络资源池，然后选择**编辑设置**。

3 为网络资源池选择**物理适配器份额**。

选项	描述
自定义	为此网络资源池输入一个特定的份额数量，从 1 到 100。
高	将此资源池的份额设置为 100。
正常	将此资源池的份额设置为 50。
低	将此资源池的份额设置为 25。

4 设置网络资源池的**主机限制**（单位：兆位/秒），或选择**无限**。

5 单击**确定**。

高级网络 5

以下主题将指导您学习 ESX 环境下的高级网络，并论述如何设置和更改高级网络配置选项。

本章讨论了以下主题：

Internet 协议版本 6

vSphere 支持 Internet 协议版本 4 (IPv4) 和 Internet 协议版本 6 (IPv6) 环境。

Internet 工程任务组已将 IPv6 指定为 IPv4 的继承者。采用 IPv6（作为独立协议使用以及在具备 IPv4 的混合环境中使用）的系统数量迅速增加。借助 IPv6，可以在 IPv6 环境中使用 vSphere 功能。

IPv4 和 IPv6 之间的主要差异是地址长度。IPv6 使用 128 位地址，而 IPv4 使用 32 位地址。这有助于缓解 IPv4 存在的地址耗尽问题并消除网络地址转换 (NAT) 的需要。其他显著的差异包括：在初始化接口时出现的链路本地地址、由路由器通告功能设置的地址以及在一个接口上使用多个 IPv6 地址的能力。

vSphere 中特定于 IPv6 的配置涉及提供 IPv6 地址，方法是通过输入静态地址或为所有相关的 vSphere 网络接口使用自动地址配置方案。

在 ESX 主机上启用 IPv6 支持

可以在主机上启用或禁用 IPv6 支持。默认情况下，IPv6 已禁用。

步骤

1. 单击导航栏中**清单**按钮旁边的箭头，然后选择**主机和群集**。
2. 选择主机，然后单击**配置**选项卡。
3. 单击“硬件”下方的**网络**链接。
4. 在“虚拟交换机”视图中，单击**属性**链接。

5 选择**在该主机上启用 IPv6 支持**，然后单击**确定**。

6 重新引导主机。

VLAN 配置

通过虚拟 LAN (VLAN)，单个物理 LAN 分段可进一步分段，以使端口组互相隔离，就好像它们位于不同物理分段上一样。

建议为 ESX 配置 VLAN，原因如下。

- 可将主机集成到预先存在的环境中。
- 可确保网络流量的安全。
- 可减少网络流量拥堵情况。
- iSCSI 流量需要一个隔离的网络。

可以使用以下三种方法在 ESX 中配置 VLAN：外部交换机标记 (EST)、虚拟交换机标记 (VST) 和虚拟客户机标记 (VGT)。

使用 EST 时，将在物理交换机上执行数据包的所有 VLAN 标记。为了访问物理交换机上的端口，会连接主机网络适配器。连接到虚拟交换机的端口组必须将其 VLAN ID 设置为 0。

使用 VST 时，在数据包离开主机之前，将由虚拟交换机执行数据包的所有 VLAN 标记。主机网络适配器必须连接到物理交换机上的中继端口。连接到虚拟交换机的端口组必须指定有适当的 VLAN ID。

使用 VGT 时，将由虚拟机执行所有 VLAN 标记。当在虚拟交换机中传入和传出帧时，虚拟机网络堆栈和外部交换机之间会保留 VLAN 标记。物理交换机端口将设置为中继端口。

注意 使用 VGT 时，必须在虚拟机上安装 802.1Q VLAN 中继驱动程序。

网络策略

在 vSwitch 或 dvPort 组级别设置的策略将应用于该 vSwitch 上的所有端口组或 dvPort 组中的 dvPort，但在端口组或 dvPort 级别被替代的配置选项除外。

可以应用下列网络策略。

- 负载平衡和故障切换
- VLAN（仅限 vNetwork 分布式交换机）
- 安全
- 流量调整
- 端口阻止策略（仅 vNetwork 分布式交换机）

负载平衡和故障切换策略

负载平衡和故障切换策略允许您确定网络流量在适配器间如何分布，以及如何在适配器发生故障时重新路由流量。

通过配置以下参数，可以编辑负载平衡和故障切换策略：

- **负载平衡策略**确定输出流量如何在分配给 vSwitch 的网络适配器之间分布。

  注意 输入流量由物理交换机上的负载平衡策略控制。

- **故障切换检测**控制链路状态和信标探测。客户机 VLAN 标记不支持信标。
- **网络适配器顺序**可以处于活动或待机状态。

在 vSwitch 上编辑故障切换和负载平衡策略

故障切换和负载平衡策略允许您确定网络流量在适配器间如何分布，以及如何在适配器发生故障时重新路由流量。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 选择 vSwitch 并单击**属性**。

4 在“vSwitch 属性”对话框中，单击**端口**选项卡。

5 要编辑 vSwitch 的“故障切换和负载平衡”值，请选择 vSwitch 项目并单击**属性**。

6 单击**网卡绑定**选项卡。

   可以在端口组级别改写故障切换顺序。默认情况下，新适配器对于所有策略都是活动的。除非您另行指定，否则新的适配器将承载 vSwitch 及其端口组的流量。

7 在“策略异常”组中指定设置。

选项	描述
负载平衡	指定如何选择上行链路。 ■ **基于源端口 ID 的路由**。根据流量进入虚拟交换机所经过的虚拟端口选择上行链路。 ■ **基于 IP 哈希的路由**。根据每个数据包的源和目标 IP 地址哈希值选择上行链路。对于非 IP 数据包，偏移量中的任何值都将用于计算哈希值。 ■ **基于源 MAC 哈希的路由**。根据源以太网哈希值选择上行链路。 ■ **使用明确故障切换顺序**。始终使用“活动适配器”列表中位于最前列的符合故障切换检测标准的上行链路。 **注意** 基于 IP 的绑定要求为物理交换机配置以太通道。对于所有其他选项，应禁用以太通道。
网络故障切换检测	指定用于故障切换检测的方法。 ■ **仅链路状态**。仅依靠网络适配器提供的链路状态。该选项可检测故障（如拨掉线缆和物理交换机电源故障），但无法检测配置错误（如物理交换机端口受跨树阻止、配置到了错误的 VLAN 中或者拔掉了物理交换机另一端的线缆）。 ■ **信标探测**。发出并侦听组中所有网卡上的信标探测，使用此信息并结合链路状态来确定链接故障。该选项可检测上述许多仅通过链路状态无法检测到的故障。
通知交换机	选择**是**或**否**指定发生故障切换时是否通知交换机。 如果选择**是**，则每当虚拟网卡连接到 vSwitch 或虚拟网卡的流量因故障切换事件而由网卡组中的其他物理网卡路由时，都将通过网络发送通知以更新物理交换机的查看表。几乎在所有情况下，为了使出现故障切换以及通过 vMotion 迁移时的延迟最短，最好使用此过程。 **注意** 当使用端口组的虚拟机正在以单播模式使用 Microsoft 网络负载平衡时，请勿使用此选项。以多播模式运行网络负载平衡时不存在此问题。

选项	描述
故障恢复	选择**是**或**否**以禁用或启用故障恢复。 此选项确定物理适配器从故障恢复后如何返回到活动的任务。如果故障恢复设置为**是**（默认值），则适配器将在恢复后立即返回到活动任务，并取代接替其位置的备用适配器（如果有）。如果故障恢复设置为**否**，那么，即使发生故障的适配器已经恢复，它仍将保持非活动状态，直到当前处于活动状态的另一个适配器发生故障并要求替换为止。
故障切换顺序	指定如何分布上行链路的工作负载。如果要使用一部分上行链路，保留另一部分来应对发生故障时的紧急情况，则可以通过将它们移到不同的组来设置此条件： ■ **活动上行链路**。当网络适配器连接正常且处于活动状态时，继续使用此上行链路。 ■ **备用上行链路**。如果其中一个活动适配器的连接中断，则使用此上行链路。 ■ **未使用的上行链路**。不使用此上行链路。

8 单击**确定**。

在端口组上编辑故障切换和负载平衡策略

故障切换和负载平衡策略允许您确定网络流量在适配器间如何分布，以及如何在适配器发生故障时重新路由流量。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 选择端口组并单击**编辑**。

4 在“属性”对话框中，单击**端口**选项卡。

5 要编辑端口组的**故障切换和负载平衡**值，请选择该端口组并单击**属性**。

6 单击**网卡绑定**选项卡。

可以在端口组级别替代故障切换顺序。默认情况下，新适配器对于所有策略都是活动的。除非您另行指定，否则新的适配器将承载 vSwitch 及其端口组的流量。

7 在“策略异常”组中指定设置。

选项	描述
负载平衡	指定如何选择上行链路。 ■ **基于源端口 ID 的路由**。根据流量进入虚拟交换机所经过的虚拟端口选择上行链路。 ■ **基于 IP 哈希的路由**。根据每个数据包的源和目标 IP 地址哈希值选择上行链路。对于非 IP 数据包，偏移量中的任何值都将用于计算哈希值。 ■ **基于源 MAC 哈希的路由**。根据源以太网哈希值选择上行链路。 ■ **使用明确故障切换顺序**。始终使用“活动适配器”列表中位于最前列的符合故障切换检测标准的上行链路。 **注意** 基于 IP 的绑定要求为物理交换机配置以太通道。对于所有其他选项，应禁用以太通道。
网络故障切换检测	指定用于故障切换检测的方法。 ■ **仅链路状态**。仅依靠网络适配器提供的链路状态。该选项可检测故障（如拔掉线缆和物理交换机电源故障），但无法检测配置错误（如物理交换机端口受跨树阻止、配置到了错误的 VLAN 中或者拔掉了物理交换机另一端的线缆）。 ■ **信标探测**。发出并侦听组中所有网卡上的信标探测，使用此信息并结合链路状态来确定链接故障。该选项可检测上述许多仅通过链路状态无法检测到的故障。

选项	描述
通知交换机	选择**是**或**否**指定发生故障切换时是否通知交换机。 如果选择**是**，则每当虚拟网卡连接到 vSwitch 或虚拟网卡的流量因故障切换事件而由网卡组中的其他物理网卡路由时，都将通过网络发送通知以更新物理交换机的查看表。几乎在所有情况下，为了使出现故障切换以及通过 vMotion 迁移时的延迟最短，最好使用此过程。 **注意** 当使用端口组的虚拟机正在以单播模式使用 Microsoft 网络负载平衡时，请勿使用此选项。以多播模式运行网络负载平衡时不存在此问题。
故障恢复	选择**是**或**否**以禁用或启用故障恢复。 此选项确定物理适配器从故障恢复后如何返回到活动的任务。如果故障恢复设置为**是**（默认值），则适配器将在恢复后立即返回到活动任务，并取代接替其位置的备用适配器（如果有）。如果故障恢复设置为**否**，那么，即使发生故障的适配器已经恢复，它仍将保持非活动状态，直到当前处于活动状态的另一个适配器发生故障并要求替换为止。
故障切换顺序	指定如何分布上行链路的工作负载。如果要使用一部分上行链路，保留另一部分来应对发生故障时的紧急情况，则可以通过将它们移到不同的组来设置此条件： ■ **活动上行链路**。当网络适配器连接正常且处于活动状态时，继续使用此上行链路。 ■ **备用上行链路**。如果其中一个活动适配器的连接中断，则使用此上行链路。 ■ **未使用的上行链路**。不使用此上行链路。

8 单击**确定**。

在 dvPort 组上编辑绑定和故障切换策略

绑定和故障切换策略允许您确定网络流量在适配器间如何分布，以及如何在适配器发生故障时重新路由流量。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 dvPort 组。

2 从“清单”菜单中，选择**网络 > 编辑设置**。

3 选择**策略**。

4 在“绑定和故障切换”组中，指定以下内容。

选项	描述
负载平衡	指定如何选择上行链路。 ■ **基于源虚拟端口的路由** - 选择基于虚拟端口的上行链路，流量正是通过此端口进入虚拟交换机。 ■ **基于 IP 哈希的路由** - 选择基于每个数据包的源和目标 IP 地址哈希值的上行链路。对于非 IP 数据包，偏移量中的任何值都将用于计算哈希值。 ■ **基于源 MAC 哈希的路由** - 选择基于源以太网哈希值的上行链路。 ■ **基于物理网卡负载的路由** - 根据当前物理网卡负载选择上行链路。 ■ **使用明确故障切换顺序** - 始终使用“活动适配器”列表中顺序最靠前的上行链路，同时传递故障切换检测标准。 **注意** 基于 IP 的绑定要求为物理交换机配置以太通道。对于所有其他选项，应禁用以太通道。
网络故障切换检测	指定用于故障切换检测的方法。 ■ **仅链路状态** – 仅依靠网络适配器提供的链路状态。该选项可检测故障（如拔掉线缆和物理交换机电源故障），但无法检测配置错误（如物理交换机端口受跨树阻止、配置到了错误的 VLAN 中或者拔掉了物理交换机另一端的线缆）。 ■ **信标探测** - 发出并侦听网卡组中所有网卡上的信标探测，使用此信息并结合链路状态来确定链路故障。该选项可检测上述许多仅通过链路状态无法检测到的故障。 **注意** 不要使用包含 IP 哈希负载平衡的信标探测。

选项	描述
通知交换机	选择**是**或**否**指定发生故障切换时是否通知交换机。 如果选择**是**，则每当虚拟网卡连接到 vSwitch 或虚拟网卡的流量因故障切换事件而由网卡组中的其他物理网卡路由时，都将通过网络发送通知以更新物理交换机的查看表。几乎在所有情况下，为了使出现故障切换以及通过 vMotion 迁移时的延迟最短，最好使用此过程。 **注意** 当使用端口组的虚拟机正在以单播模式使用 Microsoft 网络负载平衡时，请勿使用此选项。以多播模式运行网络负载平衡时不存在此问题。
故障恢复	选择**是**或**否**以禁用或启用故障恢复。 此选项确定物理适配器从故障恢复后如何返回到活动的任务。如果故障恢复设置为**是**（默认值），则适配器将在恢复后立即返回到活动任务，并取代接替其位置的备用适配器（如果有）。如果故障恢复设置为**否**，那么，即使发生故障的适配器已经恢复，它仍将保持非活动状态，直到当前处于活动状态的另一个适配器发生故障并要求替换为止。
故障切换顺序	指定如何分布上行链路的工作负载。如果要使用一部分上行链路，保留另一部分来应对发生故障时的紧急情况，则可以通过将它们移到不同的组来设置此条件： ■ **活动上行链路** - 当网络适配器连接正常且处于活动状态时继续使用该上行链路。 ■ **备用上行链路** - 如果其中一个活动适配器的连接中断，则使用此上行链路。 ■ **未使用的上行链路** - 不使用该上行链路。 **注意** 当使用 IP 哈希负载平衡时，不要配置待机上行链路。

5 单击**确定**。

编辑 dvPort 绑定和故障切换策略

绑定和故障切换策略允许您确定网络流量在适配器间如何分布，以及如何在适配器发生故障时重新路由流量。

前提条件

若要在单个 dvPort 上编辑绑定和故障切换策略，必须设置关联 dvPort 组以便允许策略替代。

步骤

1 登录到 vSphere Client，此时会显示 vNetwork 分布式交换机。

2 在**端口**选项卡上，右键单击要修改的端口，然后选择**编辑设置**。

   此时将显示**端口设置**对话框。

3 单击**策略**以查看和修改端口网络策略。

4 在“绑定和故障切换”组中，指定以下内容。

选项	描述
负载平衡	指定如何选择上行链路。 ■ **基于源虚拟端口的路由** - 选择基于虚拟端口的上行链路，流量正是通过此端口进入虚拟交换机。 ■ **基于 IP 哈希的路由** - 选择基于每个数据包的源和目标 IP 地址哈希值的上行链路。对于非 IP 数据包，偏移量中的任何值都将用于计算哈希值。 ■ **基于源 MAC 哈希的路由** - 选择基于源以太网哈希值的上行链路。 ■ **基于物理网卡负载的路由** - 根据当前物理网卡负载选择上行链路。 ■ **使用明确故障切换顺序** - 始终使用“活动适配器”列表中顺序最靠前的上行链路，同时传递故障切换检测标准。 **注意** 基于 IP 的绑定要求为物理交换机配置以太通道。对于所有其他选项，应禁用以太通道。
网络故障切换检测	指定用于故障切换检测的方法。 ■ **仅链路状态** – 仅依靠网络适配器提供的链路状态。该选项可检测故障（如拔掉线缆和物理交换机电源故障），但无法检测配置错误（如物理交换机端口受跨树阻止、配置到了错误的 VLAN 中或者拔掉了物理交换机另一端的线缆）。 ■ **信标探测** - 发出并侦听网卡组中所有网卡上的信标探测，使用此信息并结合链路状态来确定链路故障。该选项可检测上述许多仅通过链路状态无法检测到的故障。 **注意** 不要使用包含 IP 哈希负载平衡的信标探测。
通知交换机	选择**是**或**否**指定发生故障切换时是否通知交换机。 如果选择**是**，则每当虚拟网卡连接到 vSwitch 或虚拟网卡的流量因故障切换事件而由网卡组中的其他物理网卡路由时，都将通过网络发送通知以更新物理交换机的查看表。几乎在所有情况下，为了使出现故障切换以及通过 vMotion 迁移时的延迟最短，最好使用此过程。 **注意** 当使用端口组的虚拟机正在以单播模式使用 Microsoft 网络负载平衡时，请勿使用此选项。以多播模式运行网络负载平衡时不存在此问题。
故障恢复	选择**是**或**否**以禁用或启用故障恢复。 此选项确定物理适配器从故障恢复后如何返回到活动的任务。如果故障恢复设置为**是**（默认值），则适配器将在恢复后立即返回到活动任务，并取代接替其位置的备用适配器（如果有）。如果故障恢复设置为**否**，那么，即使发生故障的适配器已经恢复，它仍将保持非活动状态，直到当前处于活动状态的另一个适配器发生故障并要求替换为止。
故障切换顺序	指定如何分布上行链路的工作负载。如果要使用一部分上行链路，保留另一部分来应对发生故障时的紧急情况，则可以通过将它们移到不同的组来设置此条件： ■ **活动上行链路** - 当网络适配器连接正常且处于活动状态时继续使用该上行链路。 ■ **备用上行链路** - 如果其中一个活动适配器的连接中断，则使用此上行链路。 ■ **未使用的上行链路** - 不使用该上行链路。 **注意** 当使用 IP 哈希负载平衡时，不要配置待机上行链路。

5 单击**确定**。

VLAN 策略

VLAN 策略允许虚拟网络加入物理 VLAN。

在 dvPort 组上编辑 VLAN 策略

可以在 dvPort 组上编辑 VLAN 策略配置。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 dvPort 组。

2 从“清单”菜单中，选择**网络 > 编辑设置**。

3 选择 **VLAN**。

4 选择要使用的 **VLAN 类型**。

选项	描述
无	不使用 VLAN。
VLAN	在 **VLAN ID** 字段中，输入一个介于 1 和 4094 之间的数字。
VLAN 中继	输入 **VLAN 中继范围**。
专用 VLAN	选择可供使用的专用 VLAN。

编辑 dvPort VLAN 策略

在 dvPort 级别设置的 VLAN 策略允许单个 dvPort 替代在 dvPort 组级别设置的 VLAN 策略。

前提条件

若要在单个 dvPort 上编辑 VLAN 策略，必须设置关联 dvPort 组以便允许策略替代。

步骤

1 登录到 vSphere Client，此时会显示 vNetwork 分布式交换机。

2 在**端口**选项卡上，右键单击要修改的端口，然后选择**编辑设置**。

3 单击**策略**。

4 选择要使用的 VLAN 类型。

选项	操作
无	不使用 VLAN。
VLAN	对于 VLAN ID，输入一个介于 1 和 4095 之间的数字。
VLAN 中继	输入 VLAN 中继范围。
专用 VLAN	选择可供使用的专用 VLAN。

5 单击**确定**。

安全策略

网络安全策略确定适配器如何筛选入站和出站帧。

第 2 层是数据链路层。安全策略的三大要素是杂乱模式、MAC 地址更改和伪信号。

在非杂乱模式下，客户机适配器将仅侦听转发到其自身 MAC 地址上的流量。在杂乱模式下，它可以侦听所有帧。默认情况下，客户机适配器设置为非杂乱模式。

在 vSwitch 上编辑第 2 层安全策略

通过编辑第 2 层安全策略，控制如何处理入站和出站帧。

步骤

1 登录 VMware vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 单击 vSwitch 的**属性**，以进行编辑。

4 在“属性”对话框中，单击**端口**选项卡。

5 选择 vSwitch 项目，并单击**编辑**。

6 在“属性”对话框中，单击**安全**选项卡。

默认情况下，**杂乱模式**设置为**拒绝**，而 **MAC 地址更改**和**伪信号**则设置为**接受**。

策略将应用到 vSwitch 上的所有虚拟适配器，除非虚拟适配器的端口组指定了策略异常。

7 在“策略异常”窗格中，选择是拒绝还是接受安全策略异常。

表 5–1 策略异常

模式	拒绝	接受
杂乱模式	将客户机适配器置于杂乱模式不会对适配器接收哪些帧产生任何影响。	将客户机适配器置于杂乱模式会使其检测经过 vSwitch 且由适配器所连接到的端口组的 VLAN 策略允许的所有帧。
MAC 地址更改	如果客户机操作系统将适配器的 MAC 地址更改为不同于 `.vmx` 配置文件的其他任何内容，则将丢失所有入站帧。 如果客户机操作系统将 MAC 地址重新更改为与 `.vmx` 配置文件中的 MAC 地址匹配的地址，则会再次发送入站帧。	如果客户机操作系统的 MAC 地址发生了变化，则将接收传入新 MAC 地址的帧。
伪信号	对于出站帧，如果源 MAC 地址与适配器上设置的地址不同，则将丢失这些帧。	不执行筛选，所有出站帧均可通过。

8 单击**确定**。

在端口组上编辑第 2 层安全策略异常

通过编辑第 2 层安全策略，控制如何处理入站和出站帧。

步骤

1 登录 VMware vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 单击端口组的**属性**以进行编辑。

4 在“属性”对话框中，单击**端口**选项卡。

5 选择端口组项并单击**编辑**。

6 在端口组的“属性”对话框中，单击**安全**选项卡。

默认情况下，**杂乱模式**设置为**拒绝**。**MAC 地址更改**和**伪信号**设置为**接受**。

策略异常将替代在 vSwitch 级别上设置的任何策略。

7 在“策略异常”窗格中，选择是拒绝还是接受安全策略异常。

表 5–2 策略异常

模式	拒绝	接受
杂乱模式	将客户机适配器置于杂乱模式不会对适配器接收哪些帧产生任何影响。	将客户机适配器置于杂乱模式会使其检测经过 vSwitch 且由适配器所连接到的端口组的 VLAN 策略允许的所有帧。
MAC 地址更改	如果客户机操作系统将适配器的MAC 地址更改为不同于 `.vmx` 配置文件的其他任何内容，则将丢失所有入站帧。 如果客户机操作系统将 MAC 地址重新更改为与 `.vmx` 配置文件中的MAC 地址匹配的地址，则会再次发送入站帧。	如果客户机操作系统的MAC 地址发生了变化，则将接收传入新MAC 地址的帧。
伪信号	对于出站帧，如果源 MAC 地址与适配器上设置的地址不同，则将丢失这些帧。	不执行筛选，所有出站帧均可通过。

8 单击**确定**。

在 dvPort 组上编辑安全策略

通过编辑安全策略，控制如何处理 dvPort 组的入站和出站帧。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 dvPort 组。

2 从“清单”菜单中，选择**网络 > 编辑设置**。

3 在端口组的“属性”对话框中，单击**安全**选项卡。

默认情况下，**杂乱模式**设置为**拒绝**。**MAC 地址更改**和**伪信号**设置为**接受**。

策略异常将替代在 vSwitch 级别上设置的任何策略。

4 在“策略异常”窗格中，选择是拒绝还是接受安全策略异常。

表 5–3 策略异常

模式	拒绝	接受
杂乱模式	将客户机适配器置于杂乱模式不会对适配器接收哪些帧产生任何影响。	将客户机适配器置于杂乱模式会使其检测经过 vSwitch 且由适配器所连接到的端口组的 VLAN 策略允许的所有帧。
MAC 地址更改	如果客户机操作系统将适配器的MAC 地址更改为不同于 `.vmx` 配置文件的其他任何内容，则将丢失所有入站帧。 如果客户机操作系统将 MAC 地址重新更改为与 `.vmx` 配置文件中的MAC 地址匹配的地址，则会再次发送入站帧。	如果客户机操作系统的MAC 地址发生了变化，则将接收传入新MAC 地址的帧。
伪信号	对于出站帧，如果源 MAC 地址与适配器上设置的地址不同，则将丢失这些帧。	不执行筛选，所有出站帧均可通过。

5 单击**确定**。

编辑 dvPort 安全策略

通过编辑安全策略，控制如何处理 dvPort 的入站和出站帧。

前提条件

若要在单个 dvPort 上编辑安全策略，必须设置关联 dvPort 组以便允许策略替代。

步骤

1 登录到 vSphere Client，此时会显示 vNetwork 分布式交换机。

2 在**端口**选项卡上，右键单击要修改的端口，然后选择**编辑设置**。

3 单击**策略**。

默认情况下，**杂乱模式**设置为**拒绝**，而 **MAC 地址更改**和**伪信号**则设置为**接受**。

4 在“安全”组中，选择是拒绝还是接受安全策略异常。

表 5–4 策略异常

模式	拒绝	接受
杂乱模式	将客户机适配器置于杂乱模式不会对适配器接收哪些帧产生任何影响。	将客户机适配器置于杂乱模式会使其检测经过 vSwitch 且由适配器所连接到的端口组的 VLAN 策略允许的所有帧。
MAC 地址更改	如果客户机操作系统将适配器的 MAC 地址更改为不同于 `.vmx` 配置文件的其他任何内容，则将丢失所有入站帧。 如果客户机操作系统将 MAC 地址重新更改为与 `.vmx` 配置文件中的 MAC 地址匹配的地址，则会再次发送入站帧。	如果客户机操作系统的 MAC 地址发生了变化，则将接收传入新 MAC 地址的帧。
伪信号	对于出站帧，如果源 MAC 地址与适配器上设置的地址不同，则将丢失这些帧。	不执行筛选，所有出站帧均可通过。

5 单击**确定**。

流量调整策略

流量调整策略由三个特性定义：平均带宽、带宽峰值和突发大小。可以为每个端口组和每个 dvPort 或 dvPort 组建立流量调整策略。

ESX 调整 vSwitch 上的出站网络流量以及 vNetwork 分布式交换机上的进站和出站流量。流量调整功能会限制可用于端口的网络带宽，但也可以将其配置为允许流量突发，使流量以更高的速度通过端口。

平均带宽 规定某段时间内允许通过端口的平均每秒位数，即允许的平均负载。

带宽峰值 当端口正在发送或接收流量突发时为了通过端口而允许采用的平均每秒最大传输位数。此数值会限制端口经历额外突发时所用的带宽。

突发大小 突发中所允许的最大字节数。如果设置了此参数，则在端口没有使用为其分配的所有带宽时可能会获取额外的突发。当端口所需带宽大于**平均带宽**所指定的值时，如果有额外突发可用，则可能会临时允许以更高的速度传输数据。此参数限制在额外突发中累积的字节数，使数据以更高的速度传输。

在 vSwitch 上编辑流量调整策略

使用流量调整策略以在 vSwitch 上控制带宽和突发大小。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 单击 vSwitch 的**属性**，以进行编辑。

4 在“属性”对话框中，单击**端口**选项卡。

5 选择 vSwitch 项目，并单击**编辑**。

6 在“属性”对话框中，单击**流量调整**选项卡。

  当流量调整处于禁用状态时，这些选项会显示为灰色。如果启用流量调整，可以选择性地在端口组级别覆盖所有流量调整功能。

  此策略将应用到与端口组相连的各个虚拟适配器，而不是整个 vSwitch。

  注意 带宽峰值不能小于指定的平均带宽。

选项	描述
状态	如果在**状态**字段中启用策略异常，将为与该特定端口组关联的每个虚拟适配器设置网络带宽分配量的限制。如果禁用策略，则在默认情况下，服务将能够自由、顺畅地连接到物理网络。
平均带宽	一段特定时间内的测量值。
带宽峰值	限制突发期间的最大带宽。它永远不能小于平均带宽。
突发大小	指定突发大小的值，以千字节 (KB) 为单位。

在端口组上编辑流量调整策略

使用流量调整策略以在端口组上控制带宽和突发大小。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 单击端口组的**属性**以进行编辑。

4 在“属性”对话框中，单击**端口**选项卡。

5 选择端口组项并单击**编辑**。

6 在端口组的“属性”对话框中，单击**流量调整**选项卡。

  当流量调整处于禁用状态时，这些选项会显示为灰色。

选项	描述
状态	如果在**状态**字段中启用策略异常，将为与该特定端口组关联的每个虚拟适配器设置网络带宽分配量的限制。如果禁用策略，则在默认情况下，服务将能够自由、顺畅地连接到物理网络。
平均带宽	一段特定时间内的测量值。
带宽峰值	限制突发期间的最大带宽。它永远不能小于平均带宽。
突发大小	指定突发大小的值，以千字节 (KB) 为单位。

在 dvPort 组上编辑流量调整策略

可以调整 vNetwork 分布式交换机上的输入和输出流量。可以限制端口的可用网络带宽，但也可以临时允许流量突发，使流量以更高的速度通过端口。

流量调整策略由三个特性定义：平均带宽、带宽峰值和突发大小。流量调整策略不适用于从属硬件 iSCSI 适配器上的 iSCSI 流量。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 dvPort 组。

2 从“清单”菜单中，选择**网络 > 编辑设置**。

3 选择**流量调整**。

4 在端口组的“属性”对话框中，单击**流量调整**选项卡。

  可以配置输入流量调整和输出流量调整。当流量调整处于禁用状态时，这些选项会显示为灰色。

  注意 带宽峰值不能小于指定的平均带宽。

选项	描述
状态	如果在**状态**字段中启用策略异常，将为与该特定端口组关联的每个虚拟适配器设置网络带宽分配量的限制。如果禁用策略，则在默认情况下，服务将能够自由、顺畅地连接到物理网络。
平均带宽	一段特定时间内的测量值。
带宽峰值	限制突发期间的最大带宽。它永远不能小于平均带宽。
突发大小	指定突发大小的值，以千字节 (KB) 为单位。

编辑 dvPort 流量调整策略

可以调整 vNetwork 分布式交换机上的输入和输出流量。可以限制端口的可用网络带宽，但也可以临时允许流量突发，使流量以更高的速度通过端口。

流量调整策略由三个特性定义：平均带宽、带宽峰值和突发大小。流量调整策略不适用于从属硬件 iSCSI 适配器上的 iSCSI 流量。

前提条件

若要在单个 dvPort 上编辑流量调整策略，必须设置关联 dvPort 组以便允许策略替代。

步骤

1 登录到 vSphere Client，此时会显示 vNetwork 分布式交换机。

2 在**端口**选项卡上，右键单击要修改的端口，然后选择**编辑设置**。

3 单击**策略**。

4 在“流量调整”组中，您可以配置输入流量调整和输出流量调整。

  当流量调整处于禁用状态时，这些选项会显示为灰色。

选项	描述
状态	如果在**状态**字段中启用策略异常，将为与该特定端口组关联的每个虚拟适配器设置网络带宽分配量的限制。如果禁用策略，则在默认情况下，服务将能够自由、顺畅地连接到物理网络。
平均带宽	一段特定时间内的测量值。

选项	描述
带宽峰值	限制突发期间的最大带宽。它永远不能小于平均带宽。
突发大小	指定突发大小的值，以千字节 (KB) 为单位。

5 单击**确定**。

端口阻止策略

从“其他策略”对话框中设置 dvPorts 的阻止策略。

在 dvPort 组上编辑端口阻止策略

在其他策略下设置 dvPort 组的端口阻止策略。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 dvPort 组。
2 从“清单”菜单中，选择**网络 > 编辑设置**。
3 选择**其他**。
4 选择是否在此 dvPort 组上**阻止所有端口**。

编辑 dvPort 端口阻止策略

“其他策略”对话框允许您配置 dvPort 的端口阻止策略。

步骤

1 登录到 vSphere Client，此时会显示 vNetwork 分布式交换机。
2 在**端口**选项卡上，右键单击要修改的端口，然后选择**编辑设置**。
3 单击**策略**。
4 在**其他**组中，选择是否**阻止所有端口**。
5 单击**确定**。

更改 DNS 和路由配置

可以在 vSphere Client 中的“主机配置”页面更改安装期间提供的 DNS 服务器和默认网关信息。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。
2 依次单击**配置**选项卡和 **DNS 和路由**。
3 在窗口的右侧，单击**属性**。
4 在 **DNS 配置**选项卡中，输入名称和域。
5 选择是自动获取 DNS 服务器地址，还是使用 DNS 服务器地址。

注意 仅当服务控制台可访问 DHCP 服务器时，DHCP 才是受支持的。服务控制台必须配置了虚拟界面 (vswif) 并且附加至 DHCP 服务器所在的网络。

6 指定用于查找主机的域。

7 在**路由**选项卡中，根据需要更改默认的网关信息。

只有当将服务控制台配置为连接到多个子网时才选择网关设备。

8 单击**确定**。

MAC 地址

MAC 地址是针对服务控制台、VMkernel 和虚拟机所使用的虚拟网络适配器而生成的。

大多数情况下，生成的 MAC 地址都是合适的。但是，在以下情况下，可能需要为虚拟网络适配器设置 MAC 地址：

- 不同物理主机上的虚拟网络适配器由于共享同一子网且分配了相同的 MAC 地址而发生冲突。
- 在这种情况下，请确保虚拟网络适配器始终拥有同一个 MAC 地址。

要规避每个物理机 256 个虚拟网络适配器的限制，以及在虚拟机之间可能发生的冲突，系统管理员可以手动分配 MAC 地址。VMware 将组织唯一标识符 (OUI) 00:50:56 用于手动生成的地址。

MAC 地址的范围是 `00:50:56:00:00:00–00:50:56:3F:FF:FF`。

可以通过将下面的行添加到虚拟机配置文件中以设置地址：

```
ethernet<number>.address = 00:50:56:XX:YY:ZZ
```

其中，<*number*> 表示以太网适配器的数量，`XX` 是 00 至 3F 间有效的十六进制数字，而 `YY` 和 `ZZ` 是 00 和 FF 之间有效的十六进制数字。但 `XX` 的值不得大于 3F，以避免与 VMware Workstation 和 VMware Server 产品生成的 MAC 地址冲突。对于手动生成的 MAC 地址，其最大值为：

```
ethernet<number>.address = 00:50:56:3F:FF:FF
```

同时，必须在虚拟机配置文件中设置选项：

```
ethernet<number>.addressType="static"
```

由于 VMware ESX 虚拟机不支持任意 MAC 地址，因此必须使用以上格式。只要在硬编码的地址中为 `XX:YY:ZZ` 选择了唯一值，则在自动分配的 MAC 地址与手动分配的地址之间应该绝不会发生冲突。

MAC 地址生成

虚拟机中的每个虚拟网络适配器都被分配一个唯一的 MAC 地址。 每一家网络适配器的制造商都分配了一个唯一的名为组织唯一标识符 (OUI) 的 3 字节前缀，此标识符可用于生成唯一的 MAC 地址。

VMware 有以下 OUI：

- 生成的 MAC 地址
- 手动设置 MAC 地址
- 对于旧版虚拟机，ESX 已经不再使用。

为每个虚拟网络适配器生成的 MAC 地址的前 3 个字节由该 OUI 组成。此 MAC 地址生成算法将计算其余 3 个字节。此算法保证 MAC 地址在计算机中是唯一的，并尝试在计算机之间提供唯一的 MAC 地址。

在同一子网中，每个虚拟机的网络适配器都拥有唯一的 MAC 地址。否则，网络适配器会行为异常。该算法会随机地为任何给定主机上的运行的虚拟机和挂起的虚拟机设置一个限制值。当不同物理机上的虚拟机共享一个子网时，该算法也不会处理所有地址。

VMware 通用唯一标识符 (UUID) 生成的 MAC 地址已经通过冲突检查。所生成的 MAC 地址是使用三个部分创建的：VMware OUI、ESX 物理机的 SMBIOS UUID，以及基于（为其生成 MAC 地址）实体名称的哈希值。

在生成 MAC 地址后，除非虚拟机移动到其他位置（例如移动到同一服务器上的其他路径），否则地址不会更改。虚拟机配置文件中的 MAC 地址将被保存。在特定物理机上，已分配给运行中和已挂起虚拟机的网络适配器的所有 MAC 地址不会被跟踪。

已关闭虚拟机的 MAC 地址不会对照运行中或已挂起虚拟机的 MAC 地址进行检查。虚拟机再次启动后，有可能获得不同的 MAC 地址。获取不同地址的原因在于，与在该虚拟机此前关闭时已启动的虚拟机发生了冲突。

设置 MAC 地址

可以将静态 MAC 地址分配给已关闭虚拟机的虚拟网卡。

步骤

1 登录 vSphere Client，在“清单”面板中选择虚拟机。

2 单击**摘要**选项卡，然后单击**编辑设置**。

3 从“硬件”列表中选择网络适配器。

4 在“MAC 地址”组中，选择**手动**。

5 输入静态 MAC 地址，然后单击**确定**。

TCP 分段清除和巨帧

必须使用命令行界面在主机级别启用巨帧，以配置每个 vSwitch 的 MTU 大小。TCP 分段清除 (TSO) 在 Vmkernel 接口上默认启用，但必须在虚拟机级别启用。

启用 TSO

要在虚拟机级别启用 TSO，必须将现有 vmxnet 或可变虚拟网络适配器替换为增强型 vmxnet 虚拟网络适配器。这种替换可能会导致虚拟网络适配器的 MAC 地址发生变化。

通过增强型 vmxnet 网络适配器实现的 TSO 支持可用于运行以下客户机操作系统的虚拟机：

- 带 Service Pack 2 的 Microsoft Windows 2003 Enterprise Edition（32 位和 64 位）
- Red Hat Enterprise Linux 4（64 位）
- Red Hat Enterprise Linux 5（32 位和 64 位）
- SUSE Linux Enterprise Server 10（32 位和 64 位）

为虚拟机启用 TSO 支持

通过使用虚拟机的增强型 vmxnet 适配器，可以在该虚拟机上启用 TSO 支持。

步骤

1 登录 vSphere Client，在“清单”面板中选择虚拟机。

2 单击**摘要**选项卡，然后单击**编辑设置**。

3 从“硬件”列表中选择网络适配器。

4 记录网络适配器所使用的网络设置和 MAC 地址。

5 单击**移除**将该网络适配器从虚拟机中移除。

6 单击**添加**。

7 选择**以太网适配器**，然后单击**下一步**。

8 在“适配器类型”组中，选择 **vmxnet (增强型)**。

9 选择旧网络适配器所使用的网络设置和 MAC 地址，然后单击**下一步**。

10 单击**完成**，然后单击**确定**。

11 如果未将虚拟机设置为在每次开机时都升级 VMware Tools，则必须手动升级 VMware Tools。

TSO 在 VMkernel 接口上处于启用状态。如果对特定 VMkernel 接口禁用了 TSO，则启用 TSO 的唯一方式是删除此 VMkernel 接口，然后重新创建已启用 TSO 的 VMkernel 接口。

检查是否已在 VMkernel 接口上启用 TSO

可以检查是否在特定的 VMkernel 网络接口上启用了 TSO。

步骤

1 登录 ESX 主机的控制台。

2 使用 `esxcfg-vmknic -l` 命令显示 VMkernel 接口的列表。

列表显示每个已启用 TSO 且 TSO MSS 设置为 65535 的 VMkernel 接口。

下一步

如果未对特定的 VMkernel 接口启用 TSO，则启用 TSO 的唯一方式就是删除并重新创建该 VMkernel 接口。

启用巨帧

巨帧允许 ESX 将较大的帧发送到物理网络上。网络必须端到端支持巨帧。

最大可支持 9 KB（9000 字节）的巨帧。

必须在 ESX 主机上通过命令行界面对每个 vSwitch 或 VMkernel 接口启用巨帧。在启用巨帧之前，请与硬件供应商核对，确保您的物理网络适配器支持巨帧。

创建已启用巨帧的 vSwitch

通过更改 vSwitch 的 MTU 大小将该 vSwitch 配置为使用巨帧。

步骤

1 使用 VMware vSphere CLI 中的 `vicfg-vswitch -m <MTU> <vSwitch>` 命令为 vSwitch 设置 MTU 大小。

通过此命令，可为此 vSwitch 上的所有上行链路设置 MTU。将 MTU 大小设置为在与 vSwitch 相连的所有虚拟网络适配器中是最大的。

2 使用 `vicfg-vswitch -l` 命令在主机上显示 vSwitch 列表，并检查 vSwitch 的配置是否正确。

在 vNetwork 分布式交换机上启用巨帧

通过更改 vNetwork 分布式交换机的 MTU 大小为 vNetwork 分布式交换机启用巨帧。

步骤

1 在 vSphere Client 中，显示“网络”清单视图，并选择 vNetwork 分布式交换机。

2 从“清单”菜单中，选择 **vNetwork 分布式交换机 > 编辑设置**。

3 在**属性**选项卡上，选择**高级**。

4 将**最大 MTU** 设置为连接到 vNetwork 分布式交换机的所有虚拟网络适配器中最大的 MTU 大小，然后单击**确定**。

在虚拟机上启用巨帧支持

要在虚拟机上启用巨帧支持，该虚拟机需要增强型 vmxnet 适配器。

步骤

1 登录 vSphere Client，在“清单”面板中选择虚拟机。

2 单击**摘要**选项卡，然后单击**编辑设置**。

3 从“硬件”列表中选择网络适配器。

4 记录网络适配器所使用的网络设置和 MAC 地址。

5 单击**移除**将该网络适配器从虚拟机中移除。

6 单击**添加**。

7 选择**以太网适配器**，然后单击**下一步**。

8 在“适配器类型”组中，选择 **vmxnet (增强型)**。

9 选择旧网络适配器所使用的网络并单击**下一步**。

10 单击**完成**。

11 在“硬件”列表中选择新网络适配器。

12 在“MAC 地址”下，选择**手动**，并输入旧网络适配器使用的 MAC 地址。

13 单击**确定**。

14 检查增强型 vmxnet 适配器是否已连接到支持巨帧的 vSwitch。

15 在客户机操作系统中，配置网络适配器以允许巨帧。

   有关详细信息，请参见客户机操作系统的文档。

16 将所有的物理交换机以及与该虚拟机相连的任何物理机或虚拟机配置为支持巨帧。

创建已启用巨帧的 VMkernel 接口

可以创建启用巨帧的 VMkernel 网络接口。

步骤

1 登录到 ESX 主机的控制台。

2 使用 `esxcfg-vmknic -a -i <ip address> -n <netmask> -m <MTU> <port group name>` 命令创建支持巨帧的 VMkernel 连接。

3 使用 `esxcfg-vmknic -l` 命令显示 VMkernel 接口列表，检查启用了巨型帧的接口的配置是否正确。

4 检查 VMkernel 接口是否已连接启用巨帧的 vSwitch。

5 将所有的物理交换机以及与该 VMkernel 接口相连的任何物理机或虚拟机配置为支持巨帧。

NetQueue 和网络性能

ESX 中的 NetQueue 会利用一些网络适配器的功能，以多个可分别处理的接收队列的形式将网络流量传输到系统，这样可以使处理扩展到多个 CPU，从而提高接收端的网络性能。

在 ESX 主机上启用 NetQueue

NetQueue 在默认情况下处于启用状态。要在禁用 NetQueue 之后使用 NetQueue，必须重新启用它。

前提条件

请熟悉《VMware vSphere 命令行界面安装和参考指南》中有关配置网卡驱动程序的信息。

步骤

1 在 VMware vSphere CLI 中，使用命令 `vicfg-advcfg --set true VMkernel.Boot.netNetQueueEnable`。

2 通过 VMware vSphere CLI 将网卡驱动程序配置为使用 NetQueue。

3 重新引导 ESX 主机。

在 ESX 主机上禁用 NetQueue

NetQueue 在默认情况下处于启用状态。

步骤

1 在 VMware vSphere CLI 中，使用命令 `vicfg-advcfg --set false VMkernel.Boot.netNetQueueEnable`。

2 要在网卡驱动程序中禁用 NetQueue，请使用 `vicfg-module -s ""` *`module name`* 命令。

   例如，如果您使用的是 s2io 网卡驱动程序，请使用 `vicfg-module -s "" s2io`

3 重新引导主机。

VMDirectPath I/O

通过 VMDirectPath I/O，虚拟机可以使用 I/O 内存管理单元访问平台上的物理 PCI 功能。

配置了 VMDirectPath 的虚拟机不具有以下功能：

- vMotion
- 虚拟设备的热添加和热移除
- 挂起和恢复
- 记录和重放
- 容错
- 高可用性
- DRS（受限的可用性。虚拟机可以属于某个群集，但不能在主机之间迁移）

有关此配置支持的最新系统和适配器的信息，请参见硬件兼容性指南。

在主机上配置直通设备

可以在主机上配置直通网络连接设备。

步骤

1 从 vSphere Client 的“清单”面板中，选择主机。

2 在**配置**选项卡中，单击**高级设置**。

此时将显示“直通配置”页面，其中会列出所有可用的直通设备。绿色图标表示设备已启用且处于活动状态。橙色图标表示设备状况已发生变更，并且在使用设备前必须重新引导主机。

3 单击**编辑**。

4 选择要用于直通的设备，然后单击**确定**。

在虚拟机上配置 PCI 设备

可以在虚拟机上配置直通 PCI 设备。

步骤

1 从 vSphere Client 的“清单”面板中选择虚拟机。

2 从**清单**菜单中，选择**虚拟机 > 编辑设置**。

3 在**硬件**选项卡上，单击**添加**。

4 选择 **PCI 设备**，然后单击**下一步**。

5 选择要使用的直通设备，然后单击**下一步**。

6 单击**完成**。

将 VMDirectPath 设备添加到虚拟机可将内存预留设置为虚拟机的内存大小。

6 网络最佳做法、场景和故障排除

下列最佳做法、配置场景和故障排除准则提供针对常见网络配置和隐患的建议。

本章讨论了以下主题：

网络最优方法

在配置网络时，请考虑这些最优方法。

- 将网络服务彼此分开，以获得更好的安全性或更佳的性能。

  要使一组特定的虚拟机能够发挥最佳性能，请将它们置于单独的物理网卡上。这种分离方法可以使总网络工作负载的一部分更平均地分摊到多个 CPU 上。例如，隔离的虚拟机可更好地服务于来自 Web 客户端的流量。

- 通过使用 VLAN 对单个物理网络分段，或者使用单独的物理网络（后者为首选）可以满足以下推荐的操作。
  - 使服务控制台处于其自已的网络中是确保 ESX 系统安全的一个重要部分。由于服务控制台的安全漏洞将使得攻击者能够完全控制系统上运行的所有虚拟机，因此考虑服务控制台的网络连接性时应采取与考虑主机中的远程访问设备相同的方式。
  - 保证 vMotion 连接处于专用且单独的网络中是非常重要的，因为通过 vMotion 迁移时，客户机操作系统内存中的内容将通过网络进行传输。
- 将直通设备与 Linux 内核 2.6.20 或更低版本配合使用时，请避免使用 MSI 和 MSI-X 模式，因为这会明显影响性能。
- 要以物理方式分离网络服务并且专门将一组特定的网卡用于特定的网络服务，请为每种服务创建 vSwitch。如果无法实现，可以使用不同的 VLAN ID 将网络服务附加到端口组，以便在一个 vSwitch 上将它们分离开。与此同时，与网络管理员确认所选的网络或 VLAN 与环境中的其他部分是隔离开的，即没有与其相连的路由器。
- 可以在不影响虚拟机或运行于 vSwitch 后端的网络服务的前提下，在 vSwitch 中添加或移除网卡。如果移除所有正在运行的硬件，虚拟机仍可互相通信。而且，如果保留一个网卡原封不动，所有的虚拟机仍然可以与物理网络相连。
- 为了保护大部分敏感的虚拟机，请在虚拟机中部署防火墙，以便在带有上行链路（连接物理网络）的虚拟网络和无上行链路的纯虚拟网络之间路由。

挂载 NFS 卷

在 ESX 中，ESX 访问 ISO 映像（用作虚拟机的虚拟 CD-ROM）的 NFS 存储器的模型与 ESX Server 2.x 中所用的模型是不同的。

ESX 支持基于 VMkernel 的 NFS 挂载。新模型将通过 VMkernel NFS 功能将 NFS 卷与 ISO 映像一起挂载。以这种方式挂载的所有 NFS 卷均显示为 vSphere Client 中的数据存储。虚拟机配置编辑器允许您浏览服务控制台文件系统，来查找用作虚拟 CD-ROM 设备的 ISO 映像。

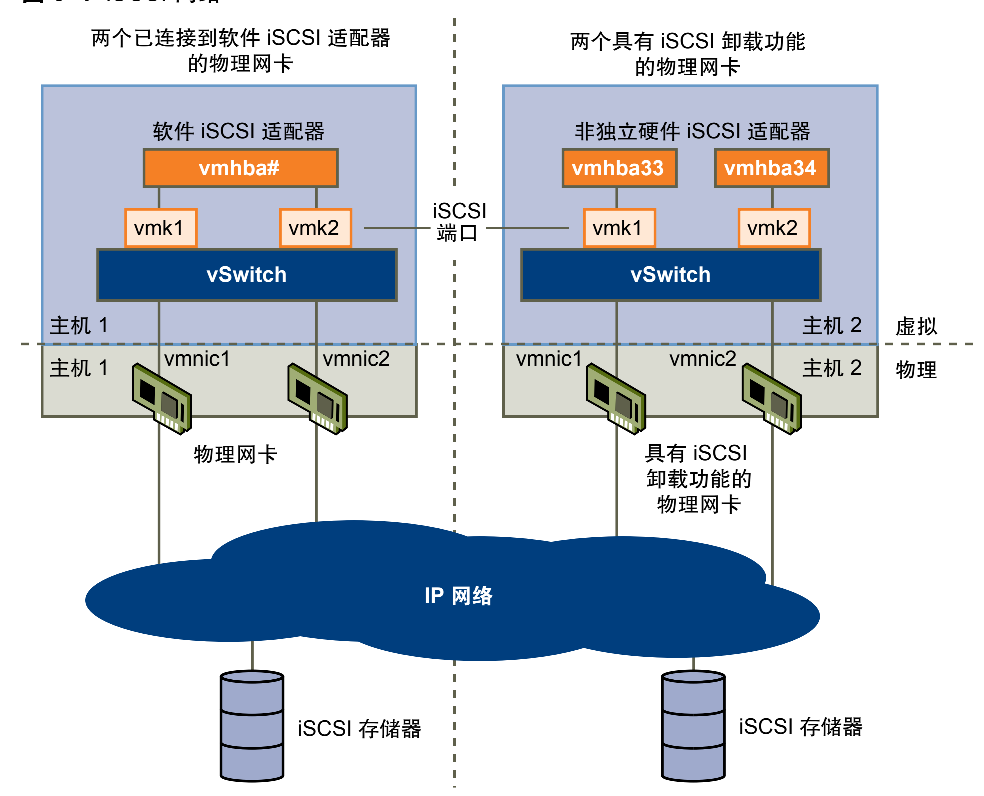
软件 iSCSI 和从属硬件 iSCSI 的网络配置

如果使用软件 iSCSI 适配器或从属硬件 iSCSI 适配器，必须先设置 iSCSI 网络，才能启用和配置 iSCSI 适配器。iSCSI 的网络配置涉及打开 VMkernel iSCSI 端口，用于 iSCSI 适配器与物理网卡之间的流量。

根据要用于 iSCSI 流量的物理网卡的数量，网络设置可能不同。

- 如果有单个物理网卡，请在与该网卡相连的 vSwitch 上创建一个 iSCSI 端口。VMware 建议为 iSCSI 指定一个单独的网络适配器。不要在 100 Mbps 或更慢的适配器上使用 iSCSI。
- 如果有两个或更多物理网卡用于 iSCSI，请为每个物理网卡创建一个单独的 iSCSI 端口，然后将这些网卡用于 iSCSI 多路径。请参见图 6‑1。

图 6‑1 iSCSI 网络



注意 使用从属硬件 iSCSI 适配器时，与该适配器关联的网卡的性能报告可能显示很少活动或无活动，即使在 iSCSI 流量很大时也是如此。出现这种行为是因为 iSCSI 流量绕过常规网络堆栈。

为单个网卡创建 iSCSI 端口

使用此任务可将运行 iSCSI 存储器服务的 VMkernel 连接至物理网卡。如果只有一个物理网络适配器要用于 iSCSI 流量，则这是设置 iSCSI 网络所必须执行的唯一过程。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。
2 依次单击**配置**选项卡和**网络**。
3 在“虚拟交换机”视图中，单击**添加网络**。
4 选择 **VMkernel**，然后单击**下一步**。
5 选择**创建虚拟交换机**以创建新的 vSwitch。
6 选择要用于 iSCSI 流量的网卡。

重要事项 如果要为从属硬件 iSCSI 适配器创建一个端口，请确保选择与 iSCSI 组件相对应的网卡。请参见第 91 页，“确定从属硬件 iSCSI 与物理网络适配器之间的关联”。

7 单击**下一步**。
8 输入网络标签。

网络标签是用于识别所创建的 VMkernel 端口的友好名称，如 iSCSI。

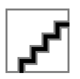
9 单击**下一步**。
10 指定 IP 设置，然后单击**下一步**。
11 检查信息，然后单击**完成**。

将多个网卡用于软件和从属硬件 iSCSI

如果主机有多个物理网卡用于 iSCSI，请使用 1:1 映射对每个物理网卡创建一个单独的 iSCSI 端口。

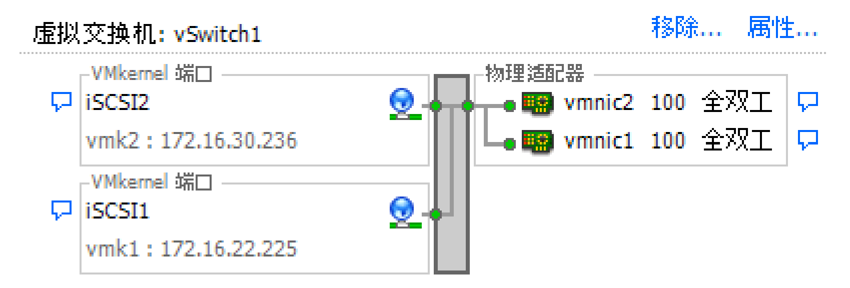
要实现 1:1 映射，请为每个网络适配器和 iSCSI 端口对指定一个单独的 vSwitch。请参见图 6‑2。

图 6‑2 单独的 vSwitch 上的 iSCSI 端口和网卡



替代方法是将所有网卡和 iSCSI 端口对添加到单个 vSwitch。请参见图 6‑3。必须替代默认设置，并确保每个端口只映射到一个对应的活动网卡。

图 6‑3 单个 vSwitch 上的 iSCSI 端口和网卡



有关将网卡和 VMkernel 端口对添加到 vSwitch 的详细信息，请参见第 66 页，“为多个网卡创建其他 iSCSI 端口”。

在将 iSCSI 端口映射到网络适配器之后，请使用 `esxcli` 命令将这些端口绑定到 iSCSI 适配器。对于从属硬件 iSCSI 适配器，无论您是使用一个网卡还是多个网卡，都要执行端口绑定。有关信息，请参见第 92 页，“将 iSCSI 端口绑定到 iSCSI 适配器”。

为多个网卡创建其他 iSCSI 端口

如果您有两个或更多个网卡可指定给 iSCSI，而且希望将所有 iSCSI 网卡连接到单个 vSwitch，请使用此任务。在此任务中，需要使用 1:1 映射将 VMkernel iSCSI 端口与网络适配器相关联。

现在需要将额外的网卡连接到现有 vSwitch，并将它们映射到相应的 iSCSI 端口。

注意 如果将具有多个 dvUplink 的 vNetwork 分布式交换机用于端口绑定，则需要为每个物理网卡创建一个单独的 dvPort 组。然后，应设置绑定策略，以便每个 dvPort 组只有一个活动 dvUplink。

有关 vNetwork 分布式交换机的详细信息，请参见“网络”部分。

前提条件

必须创建 vSwitch，将 iSCSI 端口映射到指定用于 iSCSI 流量的物理网卡。

步骤

1. 登录 vSphere Client，在“清单”面板中选择主机。
2. 依次单击**配置**选项卡和**网络**。
3. 选择用于 iSCSI 的 vSwitch，然后单击**属性**。
4. 将额外网络适配器连接到 vSwitch。
   a. 在“vSwitch 属性”对话框中，单击**网络适配器**选项卡，然后单击**添加**。
   b. 在列表中选择一个或多个网卡，然后单击**下一步**。

      对于从属硬件 iSCSI 适配器，确保只选择具有一个相应的 iSCSI 组件的那些网卡。
   c. 检查“适配器摘要”页面上的信息，然后单击**完成**。

      此时将重新出现网络适配器列表，显示现在由 vSwitch 声明的网络适配器。
5. 为已连接的所有网卡创建 iSCSI 端口。

   iSCSI 端口的数量必须与 vSwitch 上网卡的数量相对应。
   a. 在“vSwitch 属性”对话框中，单击**端口**选项卡，然后单击**添加**。
   b. 选择 **VMkernel**，然后单击**下一步**。
   c. 在**端口组属性**下方，输入网络标签（如 iSCSI），然后单击**下一步**。
   d. 指定 IP 设置，然后单击**下一步**。

      输入子网掩码时，请确保网卡已设置为其连接到的存储系统的子网。
   e. 检查信息，然后单击**完成**。


小心 如果和 iSCSI 适配器（软件或从属硬件 iSCSI 适配器）配合使用的网卡与 iSCSI 目标不在同一子网中，则主机将无法建立从此网络适配器到目标的会话。

---

6 将每个 iSCSI 端口仅映射到一个活动网卡。

   默认情况下，对于 vSwitch 上的每个 iSCSI 端口，所有网络适配器均显示为活动状态。必须替代此设置，以便每个端口只映射到一个相应的活动网卡。例如，iSCSI 端口 vmk1 映射到 vmnic1，端口 vmk2 映射到 vmnic2，等等。

   a 在**端口**选项卡上，选择 iSCSI 端口，然后单击**编辑**。

   b 单击**网卡绑定**选项卡，并选择**替代 vSwitch 故障切换顺序**。

   c 仅将一个适配器指定为活动适配器，并将所有剩余的适配器移动到**未用的适配器**类别。

7 对 vSwitch 上的每个 iSCSI 端口重复最后一步。

下一步

执行此任务后，需要使用 `esxcli` 命令将 iSCSI 端口绑定到软件 iSCSI 或从属硬件 iSCSI 适配器。

在刀片服务器上配置网络

由于刀片服务器的网络适配器数量可能有限，因此，可能需要使用 VLAN 来分离服务控制台、vMotion、IP 存储器和各组虚拟机的流量。

为安全起见，VMware 最佳做法建议为服务控制台和 vMotion 配备各自的网络。如果出于此目的将物理适配器专用于分离 vSwitch，则可能需要放弃冗余（绑定）连接，停止隔离各个网络客户端，或同时执行二者。借助 VLAN，不必使用多个物理适配器即可实现网络分段。

要使刀片服务器的网络刀片支持 ESX 端口组进行带标记的 VLAN 通信，必须将此刀片服务器配置为支持 802.1Q，将端口配置为带标记端口。

将端口配置为标记端口的方法因服务器而异。下表描述如何在三个最常用的刀片服务器上配置带标记的端口。

表 6–1 刀片服务器上的端口标记选项

服务器类型	配置选项
HP 刀片	将 **VLAN 标记**设置为**已启用**。
Dell PowerEdge	将端口设置为**已标记**。
IBM eServer 刀片中心	在端口配置中选择**标记**。

通过刀片服务器上的 VLAN 配置虚拟机端口组

在刀片服务器上配置虚拟机网络连接有一些特殊注意事项。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 在页面的右侧，单击与服务控制台相关联的 vSwitch 的**属性**。

4 在**端口**选项卡上，单击**添加**。

5 选择**虚拟机**连接类型（默认）。

6 单击**下一步**。

7 在“端口组属性”组中，输入用于标识所创建的端口组的网络标签。

   网络标签用于标识两个或多个主机共有且与迁移兼容的连接。

8 对于 **VLAN ID**，输入一个介于 1 和 4094 之间的数字。

   如果对要输入的内容不确定，请将此字段留空或向网络管理员咨询。

9 单击**下一步**。

10 确定 vSwitch 配置正确之后，单击**完成**。

通过刀片服务器上的 VLAN 配置 VMkernel 端口

可以使用刀片服务器上的 VLAN 配置 VMkernel 网络接口。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 依次单击**配置**选项卡和**网络**。

3 在页面的右侧，单击与服务控制台相关联的 vSwitch 的**属性**。

4 在**端口**选项卡上，单击**添加**。

5 选择 **VMkernel**，然后单击**下一步**。

   通过此选项，可以将物理网络连接到为 vMotion 和 IP 存储器（NFS 或 iSCSI）运行服务的 VMkernel。

6 在“端口组属性”组，选择或输入网络标签和 VLAN ID。

   输入网络标签以标识正在创建的端口组。此标签是在配置 VMkernel 服务（如 vMotion 和 IP 存储器）的过程中，配置要连接到此端口组的虚拟适配器时指定的。

   输入 VLAN ID 以标识端口组网络流量将使用的 VLAN。

7 选择**将此端口组用于 vMotion**，以便允许此端口组对另一个 ESX 主机将其自身通告为应在其中发送 vMotion 流量的网络连接。

   对于每个 ESX 主机来说，只能为其中一个 vMotion 和 IP 存储器端口组启用此属性。如果没有为任何端口组启用此属性，则无法通过 vMotion 向此主机进行迁移。

8 在“IP 设置”组中，单击**编辑**以设置 VMkernel 服务（如 vMotion、NAS 和 iSCSI）的 VMkernel 默认网关。

   在 **DNS 配置**选项卡下方，默认情况下，在名称字段中输入主机名称。在安装期间指定的 DNS 服务器地址和域也预先选定。

   在**路由**选项卡中，服务控制台和 VMkernel 均需要其自身的网关信息。连接与服务控制台或 VMkernel 位于不同 IP 子网上的计算机时，需要网关。

   静态 IP 设置为默认值。

9 单击**确定**，然后单击**下一步**。

10 单击**上一步**进行更改。

11 检查在“即将完成”页面上做出的更改，然后单击**完成**。

故障排除

您可能会遇到需要进行故障排除的主机网络问题。在许多情况下，只更改几个配置就可以还原主机网络。

服务控制台网络故障排除

如果服务控制台网络的某些部分配置错误，则无法通过 vSphere Client 访问 ESX 主机。

如果主机的服务控制台丢失网络连接，则可以通过直接连接到服务控制台并使用以下服务控制台命令来重新配置网络：

- esxcfg-vswif -l

  提供服务控制台的当前网络接口的列表。检查是否显示 vswif0 以及当前的 IP 地址和子网掩码是否正确。

- esxcfg-vswitch -l

  提供当前虚拟交换机配置的列表。检查为服务控制台配置的上行链路适配器是否连接合适的物理网络。

- exscfg-nics -l

  提供当前网络适配器的列表。检查为服务控制台配置的上行链路适配器是否为上行，且其速度和双工是否都正确。

- esxcfg-nics -s <speed> <nic>

  可更改网络适配器的速度。

- esxcfg-nics -d <duplex> <nic>

  可更改网络适配器的双工。

- esxcfg-vswif -I <new ip address> vswifX

  可更改服务控制台的 IP 地址。

- esxcfg-vswif -n <new netmask> vswifX

  可更改服务控制台的子网掩码。

- esxcfg-vswitch -U <old vmnic> <service console vswitch>

  可移除服务控制台的上行链路。

- esxcfg-vswitch -L <new vmnic> <service console vswitch>

  可更改服务控制台的上行链路。

如果使用 esxcfg-* 命令时出现长时间等待现象，则可能表明 DNS 的配置有误。esxcfg-* 命令要求配置 DNS，以便使 localhost 名称解析正常运行。这要求 /etc/hosts 文件包含适用于已配置的 IP 地址和 127.0.0.1 localhost 地址的条目。

通过使用服务控制台重命名网络适配器

如果在添加新的网络适配器之后失去了服务控制台连接，则必须使用服务控制台重命名受影响的网络适配器。添加新网络适配器可能导致无法使用 vSphere Client 对服务控制台进行连接和管理，这是因为网络适配器已重命名。

步骤

1 直接登录 ESX 主机的控制台。

2 使用 esxcfg-nics -l 命令查看已分配至网络适配器的名称。

3 使用 esxcfg-vswitch -l 命令查看与不再通过 esxcfg-nics 命令所显示的设备名称相关联的 vSwitch。

4 使用 `esxcfg-vswitch –U <old vmnic name> <vswitch>` 命令移除已重命名的任何网络适配器。

5 使用 `esxcfg-vswitch –L <new vmnic name> <vswitch>` 命令再次添加并正确命名网络适配器。

物理交换机配置故障排除

发生故障切换或故障恢复事件时，可能会丢失 vSwitch 连接。这会导致与该 vSwitch 相关联的虚拟机所使用的 MAC 地址出现在其他交换机端口上。

为了避免此问题，请将物理交换机置于 PortFast 或 PortFast 中继模式。

端口组配置故障排除

更改虚拟机所连接到的端口组的名称可能会引起已配置为连接到此端口组的虚拟机的网络配置无效。

虚拟网络适配器与端口组之间通过名称进行连接，此名称是指存储在虚拟机配置中的标识符。更改端口组的名称不需要重新配置所有与该端口组连接的虚拟机。已启动的虚拟机在关闭之前将继续运行，因为它们已与网络建立连接。

避免对使用中的网络进行重命名。重命名端口组后，必须使用服务控制台重新配置每一个相关联的虚拟机，以反映新的端口组名称。

存储器

存储器简介 7

本简介介绍了 ESX 的可用存储选项，并对如何配置 ESX 系统以使其可使用和管理不同类型的存储器进行了论述。

本章讨论了以下主题：

关于 ESX 存储器

ESX 存储器指的是多种物理存储系统（本地或联网）上的存储空间，主机使用该存储器存储虚拟机磁盘。

虚拟机使用虚拟硬盘来存储其操作系统、程序文件以及与其活动有关的其他数据。虚拟磁盘是一个大型物理文件或一组文件，可以像任何其他文件一样轻松地对其进行复制、移动、存档和备份。为了存储虚拟磁盘文件并且能够操作文件，主机需要专用的存储空间。

主机将多种物理存储系统上的存储空间（包括主机的内部和外部设备或联网的存储器）专门用于特定任务（如存储数据和保护数据）。

主机可以发现它有权限访问的存储设备并将它们格式化为数据存储。数据存储是一种特殊的逻辑容器，类似于文件系统；ESX 在其中放置虚拟磁盘文件和用来封装虚拟机基本组件的其他文件。数据存储部署在不同的存储设备上，它将各个存储设备的特性隐藏起来，并提供一个统一的模型来存储虚拟机文件。

使用 vSphere Client，可以在主机发现的任何存储设备上设置数据存储。此外，可以使用文件夹创建数据存储的逻辑组，以便实现组织目的并在数据存储组之间设置权限和警示。

物理存储器的类型

ESX 存储器管理过程以存储器管理员在不同存储系统上预先分配的存储空间开始。

ESX 支持下列类型的存储器：

本地存储器 将虚拟机文件存储在内部存储磁盘或直接连接的外部存储磁盘上。

联网的存储器 将虚拟机文件存储在通过直接连接或高速网络与主机相连的外部存储磁盘或阵列上。

本地存储器

本地存储器可以是位于 ESX 主机内部的内部硬盘，也可以是位于主机之外并直接通过 SAS 或 SATA 等协议连接主机的外部存储系统。

本地存储不需要存储网络即可与主机进行通信。您需要一根连接到存储单元的电缆；必要时，主机中需要有一个兼容的 HBA。

ESX 可支持各种内部或外部本地存储设备，其中包括 SCSI、IDE、SATA、USB 和 SAS 存储系统。无论使用何种存储器类型，主机都会向虚拟机隐藏物理存储器层。

注意 不能使用 IDE/ATA 驱动器来存储虚拟机。

本地存储设备不支持在多个主机之间共享。本地存储设备上的数据存储只能由一个主机访问。

由于大多数本地存储设备都不支持多个连接，因此您无法使用多个路径访问本地存储器。

联网的存储器

联网的存储器由 ESX 主机用于远程存储虚拟机文件的外部存储系统组成。通常，主机通过高速存储器网络访问这些系统。

网络存储设备将被共享。网络存储设备上的数据存储可同时由多个主机来访问。ESX 支持以下网络存储技术：

注意 不支持通过不同的传输协议（如 iSCSI 和光纤通道）同时访问同一个存储。

光纤通道 (FC) 在 FC 存储区域网络 (SAN) 上远程存储虚拟机文件。FC SAN 是一种将主机连接到高性能存储设备的专用高速网络。该网络使用光纤通道协议，将 SCSI 流量从虚拟机传输到 FC SAN 设备。

要连接到 FC SAN，您的主机应该配有光纤通道总线适配器 (HBA)。除非使用光纤通道直接连接存储器，否则需要光纤通道交换机来路由存储器流量。如果主机包含 FCoE（以太网上的光纤通道）HBA，则可以使用 IP 网络连接到共享光纤通道设备。

Internet SCSI (iSCSI) 在远程 iSCSI 存储设备上存储虚拟机文件。iSCSI 将 SCSI 存储器流量打包在 TCP/IP 协议中，使其通过标准 TCP/IP 网络（而不是专用 FC 网络）传输。通过 iSCSI 连接，主机可以充当与位于远程 iSCSI 存储系统的目标进行通信的启动器。

ESX 提供下列 iSCSI 连接类型：

硬件 iSCSI 主机通过能够卸载 iSCSI 和网络处理的第三方适配器连接到存储器。

软件 iSCSI 主机使用 VMkernel 中基于软件的 iSCSI 启动器连接到存储器。通过这种 iSCSI 连接类型，主机只需要一个标准的网络适配器来进行网络连接。

网络附加存储 (NAS) 在通过标准 TCP/IP 网络访问的远程文件服务器上存储虚拟机文件。ESX 中内置的 NFS 客户端使用网络文件系统 (NFS) 协议第 3 版来与 NAS/NFS 服务器进行通信。为了进行网络连接，主机需要一个标准的网络适配器。

共享串行连接的 SCSI (SAS) 在可向多个主机提供共享访问的直接连接的 SAS 存储系统上存储虚拟机。这种类型的访问允许多个主机访问 LUN 上的同一个 VMFS 数据存储。

支持的存储适配器

存储适配器为 ESX 主机提供到特定存储单元或网络的连接。

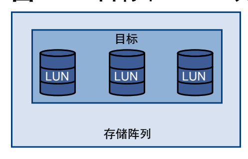
根据所使用的存储器类型，可能需要在主机上安装或启用存储适配器。ESX 支持不同的适配器类别，包括 SCSI、iSCSI、RAID、光纤通道、以太网上的光纤通道 (FCoE) 和以太网。ESX 通过 VMkernel 中的设备驱动程序直接访问适配器。

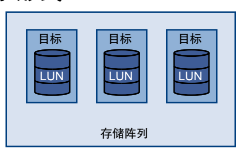
目标和设备表示形式

在 ESX 环境中，“目标”一词标识可以由主机访问的单个存储单元。术语“设备”和“LUN”描述代表目标上的存储空间的逻辑卷。通常，“设备”和“LUN”等词在 ESX 环境中表示通过存储器目标向主机呈现的 SCSI 卷，对于该卷可以格式化。

不同存储器供应商通过不同的方式向 ESX 主机呈现存储系统。某些供应商在单个目标上呈现多个存储设备或 LUN，而有些供应商则向多个目标各呈现一个 LUN。

图 7–1 目标和 LUN 表示形式





在此图示中，每种配置都有三个 LUN 可用。在其中一个示例中，主机可以看到一个目标，但该目标具有三个可供使用的 LUN。每个 LUN 表示单个存储卷。在另一个示例中，主机可以看到三个不同的目标，每个目标都拥有一个 LUN。

通过网络访问的目标都有唯一的名称，该名称由存储系统提供。iSCSI 目标使用 iSCSI 名称，而光纤通道目标使用全球名称 (WWN)。

注意 ESX 不支持通过不同传输协议（如 iSCSI 和光纤通道）访问相同的 LUN。

设备或 LUN 由其 UUID 名称标识。如果某个 LUN 由多个主机共享，则必须将该 LUN 提供给具有相同 UUID 的所有主机。

了解光纤通道命名

在光纤通道 SAN 中，全球名称 (WWN) 对网络中的每个元素（如光纤通道适配器或存储设备）进行唯一标识。

WWN 是一个由 16 个十六进制数字组成的 64 位地址，其格式如下：

```
20:00:00:e0:8b:8b:38:77 21:00:00:e0:8b:8b:38:77
```

WWN 由其制造商分配到每个光纤通道 SAN 元素。

了解 iSCSI 命名和寻址

在 iSCSI 网络中，使用网络的每个 iSCSI 元素都有一个唯一的永久 iSCSI 名称，并分配有访问地址。

iSCSI 名称

标识特定的 iSCSI 元素，而不考虑其物理位置。iSCSI 名称可以使用 IQN 或 EUI 格式。

- IQN（iSCSI 限定名）。长度可达 255 个字符，其格式如下：

  `iqn.yyyy-mm.naming-authority:unique name`

yyyy-mm	命名机构成立的年份和月份。
naming-authority	通常是命名机构的 Internet 域名的反向语法。例如，iscsi.vmware.com 命名机构的 iSCSI 限定名形式可能是 iqn.1998-01.com.vmware.iscsi。此名称表示 vmware.com 域名于 1998 年 1 月注册，iscsi 是一个由 vmware.com 维护的子域。
unique name	要使用的任何名称，例如主机名。命名机构必须确保在冒号后面分配的任何名称都是唯一的。例如 `iqn.1998-01.com.vmware.iscsi:name1`。

- EUI（扩展的唯一标识符）。包括 `eui.` 前缀，后跟 16 个字符长的名称。对于 IEEE 分配的公司名称，此名称包括 24 位；对于诸如序列号之类的唯一 ID，却包括 40 位。

  例如，

  `eui.0123456789ABCDEF`

iSCSI 别名

iSCSI 元素的一种更易管理且更便于记忆的名称，可代替 iSCSI 名称。iSCSI 别名不是唯一的，它只是一个与节点关联的友好名称。

IP 地址

地址与每个 iSCSI 元素都相关联，以便网络上的路由和交换设备可以在不同元素之间（如主机和存储器）建立连接。这就像为了访问公司的网络或 Internet 而分配给计算机的 IP 地址一样。

了解存储设备命名

在 vSphere Client 中，每个存储设备或 LUN 均由多种名称（包括友好名称、UUID 和运行时名称）标识。

名称

这是 ESX 主机根据存储器类型和制造商为设备分配的友好名称。您可以使用 vSphere Client 修改名称。当您在一台主机上修改设备的名称时，更改将在所有可以访问此设备的主机上生效。

标识符

这是分配给设备的通用唯一标识符。根据存储器类型的不同，将使用不同算法创建标识符。标识符在重新引导后仍然存在，且必须在共享设备的所有主机中相同。

运行时名称

这是设备第一条路径的名称。运行时名称由主机创建，不是设备的可靠标识符，它并不永久存在。

运行时名称具有以下格式：`vmhba#:C#:T#:L#`。

vmhba#	存储适配器的名称。此名称指的是主机上的物理适配器，而不是由虚拟机使用的 SCSI 控制器。
C#	存储通道号。软件 iSCSI 启动器使用通道号来显示指向同一目标的多个路径。
T#	目标编号。目标编号由主机决定，可能会在对于主机可见的目标的映射更改时发生变化。由不同 ESX 主机共享的目标可能具有不同的目标号。
L#	显示目标中 LUN 位置的 LUN 号。LUN 号由存储系统提供。如果目标只有一个 LUN，则 LUN 号始终为零 (0)。

例如，`vmhba1:C0:T3:L1` 表示通过存储适配器 vmhba1 和通道 0 访问的目标 3 上的 LUN 1。

关于 ESX 数据存储

数据存储是逻辑容器，类似于文件系统，它将各个存储设备的特性隐藏起来，并提供一个统一的模型来存储虚拟机文件。数据存储还可以用来存储 ISO 映像、虚拟机模板和软盘映像。

可以使用 vSphere Client 来访问 ESX 主机发现的不同类型的存储设备，并在这些设备上部署数据存储。

根据所使用的存储器类型，数据存储可以支持下面的文件系统格式：

虚拟机文件系统 (VMFS)	为存储虚拟机而优化的高性能文件系统。主机可以将 VMFS 数据存储部署在任何基于 SCSI 的本地或联网存储设备（包括光纤通道和 iSCSI SAN 设备）上。 除了使用 VMFS 数据存储之外，虚拟机还可以直接访问裸机并使用映射文件 (RDM) 作为代理。
网络文件系统 (NFS)	NAS 存储设备上的文件系统。ESX 支持 TCP/IP 上的 NFS 版本 3。主机可以访问 NAS 服务器上的指定 NFS 卷，挂载该卷，并用该卷来满足存储需求。

如果使用服务控制台访问 ESX 主机，您会看到 VMFS 和 NFS 数据存储是位于 `/vmfs/volumes` 目录下的单独子目录。

VMFS 数据存储

ESX 可以将基于 SCSI 的存储设备格式化为 VMFS 数据存储。VMFS 数据存储主要充当虚拟机的存储库。

可以在同一个 VMFS 卷上存储多个虚拟机。封装在一组文件中的各个虚拟机都会占用单独的一个目录。对于虚拟机内的操作系统，VMFS 会保留内部文件系统语义，这样可以确保正确的应用程序行为以及在虚拟机中运行的应用程序的数据完整性。

此外，还可以使用 VMFS 数据存储来存储其他文件，如虚拟机模板和 ISO 映像。

VMFS 支持下面的文件和块大小，使得虚拟机甚至能够运行会占用大量数据的应用程序（包括虚拟机中的数据库、ERP 和 CRM）：

- 最大虚拟磁盘大小：2 TB（块大小为 8 MB）
- 最大文件大小：2 TB（块大小为 8 MB）
- 块大小：1 MB（默认）、2 MB、4 MB 和 8 MB

创建和增加 VMFS 数据存储

可以在 ESX 主机发现的基于 SCSI 的任何存储设备上设置 VMFS 数据存储。创建 VMFS 数据存储以后，可以编辑它的属性。

每个系统最多可具有 256 个 VMFS 数据存储，这些数据存储的最小卷大小为 1.2GB。

注意 每个 LUN 始终只具有一个 VMFS 数据存储。

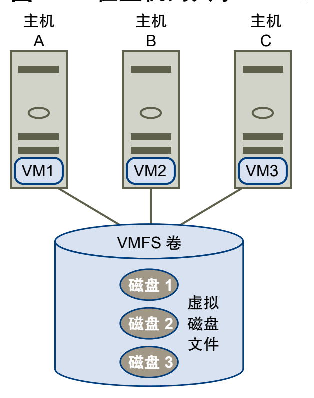
如果 VMFS 数据存储需要更多空间，则可以增加 VMFS 卷。可以将新的数据区动态添加到任何 VMFS 数据存储，该数据存储最大可达 64TB。数据区是物理存储设备上的 LUN 或分区。数据存储可以跨越多个数据区，但仍显示为单个卷。

另一个选项则是在数据存储所在的存储设备有可用空间时，增大现有的数据存储数据区。数据区最大可达 2TB。

在 ESX 主机间共享 VMFS 卷

作为一个群集文件系统，VMFS 允许多个 ESX 主机同时访问同一个 VMFS 数据存储。最多可以将 32 个主机连接到单个 VMFS 卷。

图 7–2 在主机间共享 VMFS 卷



为了确保多台服务器不会同时访问同一个虚拟机，VMFS 提供了磁盘锁定。

在多个主机间共享同一个 VMFS 卷具有以下好处：

- 可使用 VMware Distributed Resource Scheduling 和 VMware High Availability。

  可以跨越不同的物理服务器分配虚拟机。这意味着，每个服务器上会运行一组虚拟机，这样一来，所有服务器就不会同时在同一个区域面临很高的需求。如果某台服务器发生故障，可以在另一台物理服务器上重新启动虚拟机。万一发生故障，每个虚拟机的磁盘锁会被释放。

- 可以使用 vMotion 将正在运行的虚拟机从一台物理服务器移动到另一台物理服务器。
- 可以使用 VMware Consolidated Backup，它可让一个称为 VCB 代理的代理服务器在虚拟机启动和读写存储器时备份虚拟机的快照。

NFS 数据存储

ESX 可以访问 NAS 服务器上的指定 NFS 卷，挂载该卷，并用该卷来满足存储器需求。可以使用 NFS 卷来存储和引导虚拟机，这与使用 VMFS 数据存储相同。

ESX 可支持 NFS 卷上的以下共享存储器功能：

- vMotion
- VMware DRS 和 VMware HA
- 对于虚拟机显示为 CD-ROM 的 ISO 映像
- 虚拟机快照

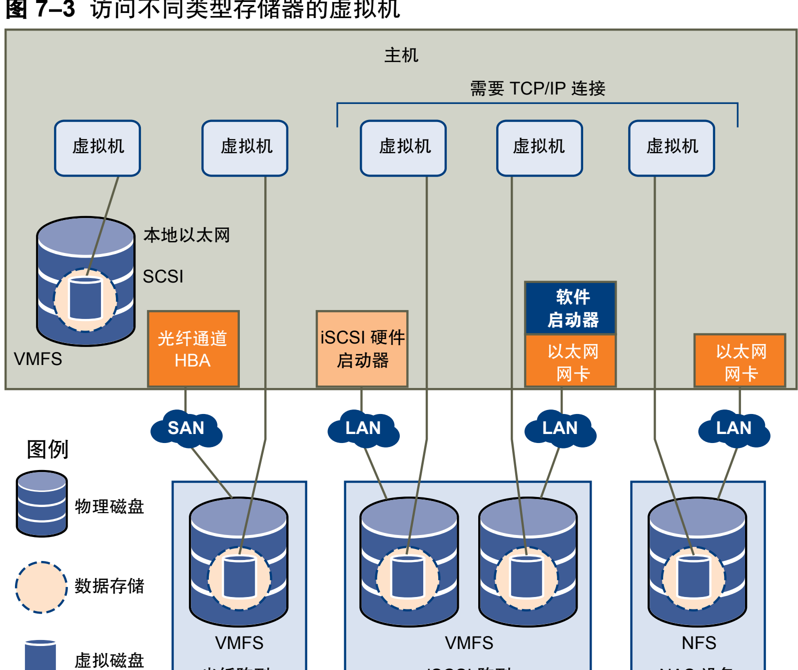
虚拟机如何访问存储器

当虚拟机与存储在数据存储上的虚拟磁盘进行通信时，它会发出 SCSI 命令。由于数据存储可以存在于各种类型的物理存储器上，因此，根据 ESX 主机用来连接存储设备的协议，这些命令会封装成其他形式。

ESX 支持光纤通道 (FC)、Internet SCSI (iSCSI)、以太网上的光纤通道 (FCoE) 和 NFS 协议。无论主机使用何种类型的存储设备，虚拟磁盘始终会以挂载的 SCSI 设备形式呈现给虚拟机。虚拟磁盘会向虚拟机操作系统隐藏物理存储器层。这样可以在虚拟机内部运行未针对特定存储设备（如 SAN）而认证的操作系统。

图 7–3 描绘了使用不同存储器类型的五个虚拟机，以说明各个类型之间的区别。

图 7–3 访问不同类型存储器的虚拟机



注意 此图表仅用于展示概念。它并非是推荐的配置。

比较存储器类型

某些 vSphere 功能是否受支持可能取决于所用存储技术。

表 7–1 比较了 ESX 支持的网络存储技术。

表 7–1 ESX 支持的联网存储器

技术	协议	传输	接口
光纤通道	FC/SCSI	数据/LUN 的块访问	FC HBA
iSCSI	IP/SCSI	数据/LUN 的块访问	■ iSCSI HBA（硬件 iSCSI） ■ 网卡（软件 iSCSI）
NAS	IP/NFS	文件（无直接 LUN 访问）	网卡

表 7–2 比较了不同类型存储器支持的 vSphere 功能。

表 7‑2 存储器支持的 vSphere 功能

存储器类型	引导虚拟机	vMotion	数据存储	RDM	虚拟机群集	VMware HA 和 DRS	VCB
本地存储器	是	否	VMFS	否	否	否	是
光纤通道	是	是	VMFS	是	是	是	是
iSCSI	是	是	VMFS	是	是	是	是
NFS 上的 NAS	是	是	NFS	否	否	是	是

显示存储适配器

主机使用存储适配器来访问不同的存储设备。您可以显示可用的存储适配器，并查看其信息。

表 7‑3 列出了在您显示每个适配器的详细信息时可以查看的信息。某些适配器（例如 iSCSI）需要对其进行配置或将其启用才能查看其适配器信息。

表 7‑3 存储适配器信息

适配器信息	描述
型号	适配器的型号。
目标（光纤通道和 SCSI）	通过适配器访问的目标数。
已连接的目标 (iSCSI)	iSCSI 适配器上已连接的目标数。
WWN（光纤通道）	根据用来唯一标识 FC 适配器的光纤通道标准形成的全球名称。
iSCSI 名称 (iSCSI)	根据用来标识 iSCSI 适配器的 iSCSI 标准形成的唯一名称。
iSCSI 别名 (iSCSI)	用以替代 iSCSI 名称的友好名称。
IP 地址（硬件 iSCSI）	分配给 iSCSI 适配器的地址。
发现方法 (iSCSI)	iSCSI 适配器用于访问 iSCSI 目标的发现方法。
设备	适配器可以访问的所有存储设备或 LUN。
路径	适配器用于访问存储设备的所有路径。

查看存储适配器信息

可以显示主机使用的存储适配器并查看它们的信息。

步骤

1 在“清单”中，选择**主机和群集**。

2 选择主机，然后单击**配置**选项卡。

3 在“硬件”中，选择**存储适配器**。

4 要查看特定适配器的详细信息，请从“存储适配器”列表中选择适配器。

5 要列出适配器可以访问的所有存储设备，请单击**设备**。

6 要列出适配器使用的所有路径，请单击**路径**。

将存储适配器标识符复制到剪贴板

如果存储适配器使用唯一标识符（如 iSCSI 名称或 WWN），则可以将标识符从 UI 直接复制到剪贴板。

步骤

1 在“清单”中，选择**主机和群集**。

2 选择主机，然后单击**配置**选项卡。

3 在“硬件”中，选择**存储适配器**。

4 从“存储适配器”列表中选择适配器。

5 在“详细信息”面板中，突出显示名称字段中的值，并从右键菜单中选择**复制**。

查看存储设备

可以显示对主机可用的所有存储设备或 LUN（包括所有的本地设备和联网设备）。如果使用第三方多路径插件，则通过此类插件可用的存储设备也将出现在列表中。

对于每个存储适配器，可以显示此适配器可用的存储设备的单独列表。

通常，在查看存储设备时，您可看到以下信息。

表 7–4 存储设备信息

存储设备信息	描述
名称	ESX 主机根据存储器类型和制造商为设备分配的友好名称。可以根据需要更改此名称。
标识符	通用唯一标识符是设备的固有名称。
运行时名称	设备第一条路径的名称。
LUN	显示目标中 LUN 位置的 LUN 号。
类型	设备类型，例如，磁盘或 CD-ROM。
传输	主机用于访问设备的传输协议。
容量	存储设备的总容量。
所有者	主机用于管理存储设备的插件（如 NMP 或第三方插件）。
硬件加速	有关存储设备是否能帮助主机执行虚拟机管理操作的信息。状态可以为“支持”、“不支持”或“未知”。有关详细信息，请参阅第 115 页，“存储硬件加速”。
位置	指向 `/vmfs/devices/` 目录中存储设备的路径。
分区	主分区和逻辑分区，包括 VMFS 数据存储（如果已配置）。

显示主机的存储设备

可以显示对主机可用的所有存储设备或 LUN。如果使用任何第三方多路径插件，则通过此类插件可用的存储设备也将出现在列表中。

步骤

1 在“清单”中，选择**主机和群集**。

2 选择主机，然后单击**配置**选项卡。

3 在“硬件”中，选择**存储器**。

4 单击**设备**。

5 要查看有关特定设备的其他详细信息，请从列表中选择设备。

显示适配器的存储设备

可以显示主机上的特定存储适配器可访问的存储设备的列表。

步骤

1 在“清单”中，选择**主机和群集**。
2 选择主机，然后单击**配置**选项卡。
3 在“硬件”中，选择**存储适配器**。
4 从“存储适配器”列表中选择适配器。
5 单击**设备**。

将存储设备标识符复制到剪贴板

存储设备标识符是分配给存储设备或 LUN 的通用唯一 ID。根据不同存储器类型使用不同的算法来创建标识符，标识符可能较长且很复杂。可以直接从 UI 复制存储设备标识符。

步骤

1 显示存储设备的列表。
2 右键单击设备，然后选择**将标识符复制到剪贴板**。

显示数据存储

可以显示对主机可用的所有数据存储，并分析其属性。

可使用以下方式将数据存储添加到 vSphere Client 中：

- 在可用存储设备上创建。
- 当主机添加到清单时发现。将主机添加到清单中时，vSphere Client 将显示对主机可用的任何数据存储。

如果 vSphere Client 连接到 vCenter Server 系统，则可以在“数据存储”视图中查看数据存储信息。此视图按数据中心显示清单中所有的数据存储。通过此视图，可以将数据存储组织到文件夹层次结构中，创建数据存储，编辑其属性，或移除现有数据存储。

此视图可全面显示数据存储的所有信息，包括使用数据存储的主机和虚拟机、存储报告信息、权限、警报、任务与事件、存储拓扑以及存储报告。“数据存储”视图的“配置”选项卡上提供连接到此数据存储的所有主机上的每个数据存储的配置详细信息。

注意 vSphere Client 直接连接到主机时，“数据存储”视图不可用。在这种情况下，通过主机存储配置选项卡检查数据存储信息。

表 7-5 说明查看数据存储时显示的数据存储详细信息。

表 7-5 数据存储信息

数据存储信息	描述
标识	分配给数据存储的可编辑名称。
设备	在其上部署数据存储的存储设备。
容量	数据存储的总格式化容量。
可用空间	可用空间。
类型	数据存储使用的文件系统，可能是 VMFS 或 NFS。
存储 I/O 控制	允许对群集范围的存储 I/O 进行优化。请参见《vSphere 资源管理指南》。

表 7–5 数据存储信息 （续）

数据存储信息	描述
硬件加速	有关数据存储是否能帮助主机执行虚拟机管理操作的信息。状态可以为“支持”、“不支持”或“未知”。有关详细信息，请参阅第 115 页，“存储硬件加速”。
位置	指向 `/vmfs/volumes/` 目录中数据存储的路径。
数据区	数据存储跨越的各个数据区及其容量（仅 VMFS 数据存储）。
路径选择	主机用于访问存储（仅限 VMFS 数据存储）的路径选择策略。
路径	用于访问存储及其状态（仅限 VMFS 数据存储）的路径数目。

检查数据存储属性

可以显示对主机可用的所有数据存储，并分析其属性。

步骤

1 显示清单中的主机。

2 在清单中选择主机，然后单击**配置**选项卡。

3 在“硬件”中，选择**存储器**。

4 单击**数据存储**视图。

5 要显示特定数据存储的详细信息，请从列表中选择数据存储。

配置 ESX 存储器 8

下列主题包含有关配置本地 SCSI 存储设备、光纤通道 SAN 存储器、iSCSI 存储器以及 NFS 存储器的信息。

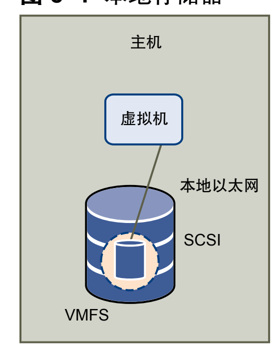
本章讨论了以下主题：

本地 SCSI 存储器

本地存储器使用基于 SCSI 的设备，如 ESX 主机的硬盘或与主机直接相连的外部专用存储系统。

图 8–1 描述了使用本地 SCSI 存储器的虚拟机。

图 8–1 本地存储器



在这个本地存储器拓扑示例中，ESX 主机使用的是到磁盘的单一连接。可以在该磁盘上创建 VMFS 数据存储，以存储虚拟机磁盘文件。

虽然可以使用这种存储器配置拓扑，但不推荐使用。如果在存储阵列和主机间使用单一连接，那么，在连接不稳定或出现故障时，会产生将导致中断的单一故障点 (SPOF)。

为确保容错性能，部分 DAS 系统支持冗余连接路径。

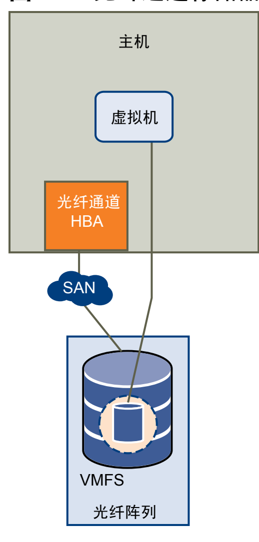
光纤通道存储器

ESX 支持光纤通道适配器，这些适配器允许主机连接到 SAN 并查看 SAN 上的存储设备。

安装光纤通道 (FC) 适配器之后，主机才能访问 FC 存储设备。

图 8‑2 描述了使用光纤通道存储器的虚拟机。

图 8–2 光纤通道存储器



在该配置中，ESX 主机通过光纤通道适配器连接到 SAN 结构（包括光纤通道交换机及存储阵列）。此时，存储阵列的 LUN 变得对于主机可用。您可以访问 LUN 并创建用于满足存储需求的数据存储。数据存储采用 VMFS 格式。

有关设置 FC SAN 光纤和存储器阵列以便与 ESX 一起使用的特定信息，请参见《光纤通道 SAN 配置指南》。

iSCSI 存储器

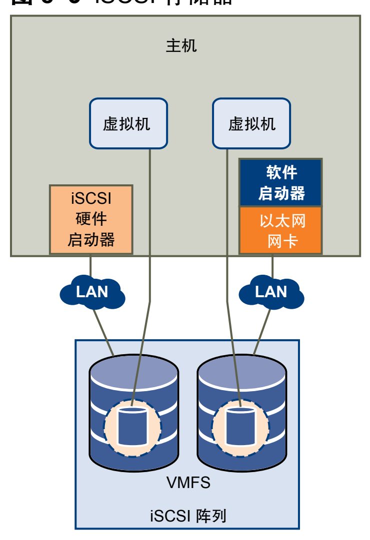
ESX 支持 iSCSI 技术，通过该技术主机可使用 IP 网络访问远程存储器。借助 iSCSI，可将虚拟机向其虚拟磁盘发出的 SCSI 存储器命令转换为 TCP/IP 数据包，并将其传输至存储虚拟磁盘的远程设备或目标。

要访问远程目标，主机需要使用 iSCSI 启动器。启动器在 IP 网络上的主机与目标存储设备之间传输 SCSI 请求和响应。ESX 支持硬件（从属和独立）和软件 iSCSI 启动器。

必须配置 iSCSI 启动器以使主机能够访问和显示 iSCSI 存储设备。

图 8‑3 描述了不同类型的 iSCSI 启动器。

图 8–3 iSCSI 存储器



在左侧示例中，主机使用硬件 iSCSI 适配器连接到 iSCSI 存储系统。

在右侧示例中，主机使用软件 iSCSI 适配器和以太网网卡连接到 iSCSI 存储器。

此时，存储系统中的 iSCSI 存储设备变得对于主机可用。您可以访问存储设备并创建用于满足存储需求的 VMFS 数据存储。

有关设置 iSCSI SAN 以便与 ESX 一起使用的特定信息，请参见《iSCSI SAN 配置指南》。

iSCSI 启动器

要访问 iSCSI 目标，主机需要使用 iSCSI 启动器。启动器在主机与 iSCSI 目标之间传输封装到 iSCSI 协议中的 SCSI 请求和响应。

VMware 支持各种类型的启动器。

软件 iSCSI 适配器

软件 iSCSI 适配器是 VMkernel 中内置的 VMware 代码。借助于该适配器，主机可通过标准网络适配器连接到 iSCSI 存储设备。软件 iSCSI 适配器可在与网络适配器进行通信的过程中负责 iSCSI 处理过程。借助软件 iSCSI 适配器，您无需购买专用硬件便可使用 iSCSI 技术。

硬件 iSCSI 适配器

硬件 iSCSI 适配器是第三方适配器，可从主机卸载 iSCSI 和网络处理。硬件 iSCSI 适配器分为几种类别。

从属硬件 iSCSI 适配器

基于 VMware 网络以及由 VMware 提供的 iSCSI 配置和管理界面。

这种类型的适配器可以是一张为同一端口提供标准网络适配器和 iSCSI 卸载功能的卡。iSCSI 卸载功能取决于主机获取 IP、MAC 和其他用于 iSCSI 会话的参数的网络配置。iSCSI 许可的 Broadcom 5709 网卡就是一种从属适配器。

独立硬件 iSCSI 适配器

执行自己的网络及 iSCSI 配置和管理界面。

只提供 iSCSI 卸载功能，或者提供 iSCSI 卸载功能和标准网卡功能的卡就是一种独立硬件 iSCSI 适配器。iSCSI 卸载功能具有独立的配置管理，可分配 IP、MAC 和其他用于 iSCSI 会话的参数。QLogic QLA4052 适配器就是一种独立适配器。

硬件 iSCSI 适配器可能需要获得许可。否则，将不会出现在 vSphere Client 或 vSphere CLI 中。有关许可信息，请联系供应商。

设置独立硬件 iSCSI 适配器

独立硬件 iSCSI 适配器是可通过 TCP/IP 访问 iSCSI 存储器的专用第三方适配器。此 iSCSI 适配器负责 ESX 系统的所有 iSCSI 以及网络处理和管理。

独立硬件 iSCSI 适配器的设置和配置过程包含以下步骤：

1 检查适配器是否需要获得许可。

请参见供应商文档。

2 安装适配器。

有关安装信息，请参见供应商文档。

3 验证适配器是否安装正确。

请参见第 88 页，“查看独立硬件 iSCSI 适配器”。

4 配置发现地址。

请参见第 93 页，“配置 iSCSI 启动器的发现地址”。

5 配置 CHAP 参数。

请参见第 94 页，“配置 iSCSI 适配器的 CHAP 参数”。

要使主机能够访问 iSCSI 存储器，必须先安装硬件 iSCSI 适配器并配置发现地址和 CHAP 参数。

查看独立硬件 iSCSI 适配器

可以查看硬件 iSCSI 适配器以验证它是否已正确安装并准备好进行配置。

前提条件

安装硬件 iSCSI 适配器后，它会显示在可供配置的存储适配器列表上。您可查看其属性。

所需特权：**主机.配置.存储器分区配置**

步骤

1 登录到 vSphere Client，然后在“清单”面板中选择主机。

2 单击**配置**选项卡，然后在“硬件”面板中单击**存储适配器**。

如果已安装，则硬件 iSCSI 启动器应显示在存储适配器列表上。

3 选择要查看的启动器。

此时会显示启动器的默认详细信息，包括型号、iSCSI 名称、iSCSI 别名、IP 地址及目标和路径信息。

4 单击**属性**。

此时将显示“iSCSI 启动器属性”对话框。**常规**选项卡显示了启动器的附加特性。

现在可配置硬件启动器或更改其默认特性。

更改独立硬件启动器的名称和 IP 地址

在配置独立硬件 iSCSI 启动器时，请确保其名称和 IP 地址的格式正确。

步骤

1 访问“iSCSI 启动器属性”对话框。

2 单击**配置**。

3 要更改启动器的默认 iSCSI 名称，请输入新的名称。

   确保所输入的名称在整个环境中唯一且其格式正确；否则，某些存储设备可能无法识别硬件 iSCSI 启动器。

4 （可选）输入 iSCSI 别名。

   别名是用于标识硬件 iSCSI 启动器的名称。

5 更改默认 IP 设置。

   必须更改默认 IP 设置，以便 IP SAN 的 IP 设置正确无误。与网络管理员一起确定 HBA 的 IP 设置。

6 单击**确定**保存更改。

如果更改 iSCSI 名称，该名称会在新的 iSCSI 会话中使用。但对于现有会话，直到注销并重新登录之后才能使用新设置。

设置和配置软件 iSCSI 适配器

借助基于软件的 iSCSI 实施，可使用标准网卡将主机连接至 IP 网络上的远程 iSCSI 目标。ESX 中内置的软件 iSCSI 适配器为此连接提供了便利，可通过网络堆栈与物理网卡进行通信。

使用 vSphere Client 连接 vCenter Server 或主机后，可以看到存储适配器列表上的软件 iSCSI 适配器。只显示一个软件 iSCSI 适配器。在使用软件 iSCSI 适配器之前，必须设置网络、启用适配器，并配置发现地址和 CHAP 等参数。软件 iSCSI 适配器配置工作流程包括以下步骤：

1 通过创建用于 iSCSI 流量的端口来配置 iSCSI 网络。

   请参见第 64 页，“软件 iSCSI 和从属硬件 iSCSI 的网络配置”。

2 启用软件 iSCSI 适配器。

   请参见第 89 页，“启用软件 iSCSI 适配器”。

3 如果将多个网卡用于软件 iSCSI 多路径，则通过将所有 iSCSI 端口连接到软件 iSCSI 适配器来执行端口绑定。

   请参见第 92 页，“将 iSCSI 端口绑定到 iSCSI 适配器”。

4 如有需要的话，请启用巨帧。必须通过 vSphere CLI 为每个 vSwitch 启用巨帧。此外，如果使用的是 ESX 主机，则必须创建已启用巨帧的 VMkernel 网络接口。

   有关详细信息，请参见“网络”部分。

5 配置发现地址。

   请参见第 93 页，“配置 iSCSI 启动器的发现地址”。

6 配置 CHAP 参数。

   请参见第 94 页，“配置 iSCSI 适配器的 CHAP 参数”。

启用软件 iSCSI 适配器

必须启用软件 iSCSI 适配器，以便主机可以使用它来访问 iSCSI 存储器。

前提条件

在启用软件 iSCSI 适配器之前，必须设置 iSCSI 的网络。

注意 如果使用软件 iSCSI 适配器从 iSCSI 进行引导，则在首次引导时会启用该适配器，并自动创建网络配置。如果禁用了该适配器，它会在您每次引导主机时重新启用。

步骤

1 登录 vSphere Client，从“清单”面板中选择服务器。

2 单击**配置**选项卡，然后在“硬件”面板中单击**存储适配器**。

此时将显示可用存储适配器的列表。

3 选择要配置的 iSCSI 启动器，然后单击**属性**。

4 单击**配置**。

5 要启用启动器，请选择**已启用**，然后单击**确定**。

启用启动器之后，主机将为其分配默认的 iSCSI 名称。如果需要您可以更改默认名称。

设置和配置从属硬件 iSCSI 适配器

从属硬件 iSCSI 适配器是基于 VMware 网络以及由 VMware 提供的 iSCSI 配置和管理界面的第三方适配器。

这种适配器类型可以是一张为同一端口提供标准网络适配器和 iSCSI 卸载功能的卡，例如 Broadcom 5709 网卡。iSCSI 卸载功能作为 iSCSI 适配器显示在存储适配器列表中。虽然默认情况下 iSCSI 适配器已启用，但若要使其正常工作，必须设置适用于 iSCSI 流量的网络，并将适配器与相应的 VMkernel iSCSI 端口绑定。然后，可以配置此适配器。

从属硬件 iSCSI 适配器的完整设置和配置过程包括以下步骤：

1 查看从属硬件适配器。

请参见第 91 页，“查看从属硬件 iSCSI 适配器”。

如果从属硬件适配器未显示在存储适配器列表中，请检查是否需要获取它们的许可。请参见供应商文档。

2 确定从属硬件适配器与物理网卡之间的关联。

请参见第 91 页，“确定从属硬件 iSCSI 与物理网络适配器之间的关联”

确保记下对应物理网卡的名称。例如，vmhba33 适配器与 vmnic1 相对应，而 vmhba34 与 vmnic2 相对应。

3 通过创建用于 iSCSI 流量的端口来配置 iSCSI 网络。

请参见第 64 页，“软件 iSCSI 和从属硬件 iSCSI 的网络配置”。

对每个网卡打开一个端口。例如，为 vmnic1 网卡创建 vmk1 端口，并为 vmnic2 创建 vmk2 端口。

4 将 iSCSI 端口绑定到对应的从属硬件 iSCSI 适配器。无论您有多个适配器还是只有一个适配器，都必须执行此步骤。

请参见第 92 页，“将 iSCSI 端口绑定到 iSCSI 适配器”。

在此示例中，将端口 vmk1 绑定到 vmhba33，并将端口 vmk2 绑定到 vmhba34。

5 配置发现地址。

请参见第 93 页，“配置 iSCSI 启动器的发现地址”。

6 配置 CHAP 参数。

请参见第 94 页，“配置 iSCSI 适配器的 CHAP 参数”。

从属硬件 iSCSI 注意事项

当将从属硬件 iSCSI 适配器与 ESX 一起使用时，某些注意事项适用。

- 使用任何从属硬件 iSCSI 适配器时，与该适配器关联的网卡的性能报告可能显示很少活动或无活动，即使在 iSCSI 流量很大时也是如此。出现这种行为是因为 iSCSI 流量绕过常规网络堆栈。
- Broadcom iSCSI 适配器在硬件中执行数据重组，其缓冲区空间有限。在拥堵的网络中或在负载下使用 Broadcom iSCSI 适配器时，启用流量控制可避免性能下降。

  流量控制可管理两个节点之间的数据传输速率，以防止发送方的速度过快而超过接收方。为了获得最佳效果，请在 I/O 路径端点处、主机和 iSCSI 存储系统上启用流量控制。
- Broadcom iSCSI 适配器不支持 IPv6 和巨帧。

查看从属硬件 iSCSI 适配器

查看从属硬件 iSCSI 适配器以验证其加载正确。

如果从属硬件适配器未显示在存储适配器列表中，请检查是否需要获取它的许可。请参见供应商文档。

步骤

1. 登录到 vSphere Client，然后在“清单”面板中选择主机。
2. 单击**配置**选项卡，然后在“硬件”面板中单击**存储适配器**。

   如果已安装，则从属硬件 iSCSI 适配器应显示在存储适配器列表中。
3. 选择要查看的适配器，然后单击**属性**。

“iSCSI 启动器属性”对话框会显示该适配器的默认详细信息，包括 iSCSI 名称和 iSCSI 别名。

确定从属硬件 iSCSI 与物理网络适配器之间的关联

需要确定与从属硬件 iSCSI 适配器关联的物理网卡的名称。还需要知道能够正确执行端口绑定的关联。

步骤

1. 使用 vSphere CLI 命令确定与 iSCSI 适配器关联的物理网卡的名称。

   ```
   esxcli swiscsi vmnic list -d vmhba#
   ```

   vmhba# 是 iSCSI 适配器的名称。
2. 在输出中，找到 `vmnic name:vmnic#` 这一行。

   vmnic# 是与 iSCSI 适配器对应的网络适配器的名称。

下一步

确定网卡的名称后，请在连接到网卡的 vSwitch 上创建一个 iSCSI 端口。然后将此端口绑定到从属硬件 iSCSI 适配器，以便您的主机可以指导通过网卡的 iSCSI 流量。

将 iSCSI 端口绑定到 iSCSI 适配器

可将为网卡创建的 iSCSI 端口绑定到 iSCSI 适配器。对于软件 iSCSI 适配器，只有在您设置了两个或更多个用于 iSCSI 多路径的网卡时，才需要执行此任务。如果使用从属硬件 iSCSI 适配器，则无论您有多个适配器还是一个适配器，都需要执行此任务。

前提条件

您可完成以下任务：

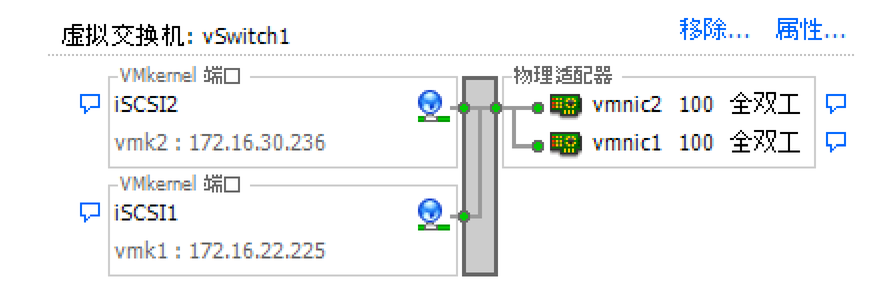
- 对于从属硬件 iSCSI 适配器，使物理网卡与 iSCSI 适配器之间正确地关联。请参见第 91 页，“查看从属硬件 iSCSI 适配器”。
- 设置用于 iSCSI 流量的网络。请参见第 64 页，“软件 iSCSI 和从属硬件 iSCSI 的网络配置”。
- 要使用软件 iSCSI 适配器，首先将它启用。请参见第 89 页，“启用软件 iSCSI 适配器”。

步骤

1 确定分配给物理网卡的 iSCSI 端口的名称。

vSphere Client 在网络标签下显示端口的名称。

在下图中，端口的名称为 vmk1 和 vmk2。



2 使用 vSphere CLI 命令将 iSCSI 端口绑定到 iSCSI 适配器。

```
esxcli swiscsi nic add -n port_name -d vmhba
```

重要事项 对于软件 iSCSI，对连接所有端口与软件 iSCSI 适配器的每个 iSCSI 端口重复此命令。对于从属硬件 iSCSI，确保将每个端口绑定到适当的相应适配器。

---

3 验证是否已将该端口添加到 iSCSI 适配器。

```
esxcli swiscsi nic list -d vmhba
```

4 使用 vSphere Client 重新扫描 iSCSI 适配器。

配置 iSCSI 启动器的发现地址

设置目标发现地址，以便 iSCSI 启动器确定网络上可供访问的存储资源。

ESX 系统支持以下发现方法：

动态发现 也称为 SendTargets 发现。启动器每次与指定的 iSCSI 服务器联系时，都会向该服务器发送 SendTargets 请求。服务器通过向启动器提供一个可用目标的列表来做出响应。这些目标的名称和 IP 地址显示在**静态发现**选项卡上。如果移除了通过动态发现添加的静态目标，则该目标可在下次进行重新扫描、重置 HBA 或重新引导主机时返回到列表中。

静态发现 启动器不必执行任何发现。启动器拥有它可以联系的目标列表，并使用目标的 IP 地址和名称与这些目标进行通信。

设置动态发现

使用动态发现时，启动器每次与指定的 iSCSI 服务器联系时，都会向该服务器发送 SendTargets 请求。服务器通过向启动器提供一个可用目标的列表来做出响应。

设置动态发现时，只能添加新的 iSCSI 服务器。不能更改现有 iSCSI 服务器的 IP 地址、DNS 名称或端口号。要进行更改，请删除现有服务器，并添加一台新服务器。

步骤

1 登录 vSphere Client，在“清单”面板中选择服务器。

2 单击**配置**选项卡，然后在“硬件”面板中单击**存储适配器**。

   此时将显示可用存储适配器的列表。

3 选择要配置的 iSCSI 启动器，然后单击**属性**。

4 在“iSCSI 启动器属性”对话框中，单击**动态发现**选项卡。

5 要为 SendTargets 发现添加地址，请单击**添加**。

   此时将显示**添加发送目标服务器**对话框。

6 输入存储系统的 IP 地址或 DNS 名称，然后单击**确定**。

   在主机与此系统建立 SendTargets 会话后，新发现的任何目标均将出现在“静态发现”列表中。

7 要删除特定的发送目标服务器，请将其选中，然后单击**移除**。

   在移除发送目标服务器之后，它可能仍作为静态目标的父目标出现在“继承”字段中。此条目表示静态目标的发现位置且并不影响功能。

下一步

为 iSCSI 适配器配置动态发现后，请重新扫描适配器。

设置静态发现

借助于 iSCSI 启动器以及动态发现方法，可以使用静态发现并手动输入目标的信息。

设置静态发现时，只能添加 iSCSI 目标。不能更改现有目标的 IP 地址、DNS 名称、iSCSI 目标名称或端口号。要进行更改，请移除现有目标，然后添加一个新目标。

步骤

1 登录 vSphere Client，在“清单”面板中选择服务器。

2 单击**配置**选项卡，然后在“硬件”面板中单击**存储适配器**。

 此时将显示可用存储适配器的列表。

3 选择要配置的 iSCSI 启动器，然后单击**属性**。

4 在“iSCSI 启动器属性”对话框中，单击**静态发现**选项卡。

 该选项卡将显示所有动态发现目标和已输入的所有静态目标。

5 要添加目标，请单击**添加**，然后输入目标的信息。

6 要删除特定目标，请选择目标，然后单击**移除**。

下一步

为 iSCSI 适配器配置静态发现后，请重新扫描适配器。

配置 iSCSI 适配器的 CHAP 参数

由于 iSCSI 技术用来连接远程目标的 IP 网络不保护其传输的数据，因此必须确保连接的安全。质询握手身份验证协议 (CHAP) 是 iSCSI 实现的协议之一，该协议会验证访问网络上目标的启动器的合法性。

在主机和目标建立连接时，CHAP 使用三路握手算法验证主机和 iSCSI 目标（如果适用的话）的身份。系统根据启动器和目标共享的预定义的专用值或 CHAP 密钥进行验证。

ESX 支持适配器级别的 CHAP 身份验证。在这种情况下，所有目标从 iSCSI 启动器接收相同的 CHAP 名称和密钥。对于软件和从属硬件 iSCSI 适配器，ESX 还支持基于每个目标的 CHAP 身份验证，此身份验证使您能够为每个目标配置不同凭据以实现更高级别的安全性。

选择 CHAP 身份验证方法

ESX 支持为所有类型的 iSCSI 启动器设置单向 CHAP，以及为软件和从属硬件 iSCSI 设置双向 CHAP。

在配置 CHAP 前，请检查是否在 iSCSI 存储系统中启用了 CHAP 并检查系统所支持的 CHAP 身份验证方法。如果已启用 CHAP，请为启动器启用 CHAP，并确保 CHAP 身份验证凭据与 iSCSI 存储器上的身份验证凭据相匹配。

ESX 支持下列 CHAP 身份验证方法：

单向 CHAP 在单向 CHAP 身份验证中，目标需验证启动器，但启动器无需验证目标。

双向 CHAP 在双向 CHAP 身份验证中，提供了供启动器验证目标的附加安全级别。VMware 仅对软件和从属硬件 iSCSI 适配器支持此方法。

对于软件和从属硬件 iSCSI 适配器，可以为每个启动器或在目标级别设置单向 CHAP 和双向 CHAP。硬件 iSCSI 仅支持启动器级别的 CHAP。

设置 CHAP 参数时，请指定 CHAP 的安全级别。

注意 指定 CHAP 安全级别时，存储阵列的响应方式取决于阵列的 CHAP 实施，且因供应商而异。例如，选择使用 CHAP，除非已被目标禁止时，有些存储阵列在响应时会使用 CHAP，而有些则不会。有关不同的启动器和目标配置中的 CHAP 身份验证行为的信息，请参阅阵列文档。

表 8–1 CHAP 安全级别

CHAP 安全级别	描述	受支持的
不使用 CHAP	主机不使用 CHAP 身份验证。如果当前已启用，则选择此选项禁用身份验证。	软件 iSCSI 从属硬件 iSCSI 独立硬件 iSCSI
不使用 CHAP，除非目标需要	主机首选非 CHAP 连接，但如果目标要求可以使用 CHAP 连接。	软件 iSCSI 从属硬件 iSCSI
使用 CHAP，除非已被目标禁止	主机首选 CHAP，但如果目标不支持 CHAP，可以使用非 CHAP 连接。	软件 iSCSI 从属硬件 iSCSI 独立硬件 iSCSI
使用 CHAP	主机需要成功的 CHAP 身份验证。如果 CHAP 协商失败，则连接失败。	软件 iSCSI 从属硬件 iSCSI

设置 iSCSI 启动器的 CHAP 凭据

您可以在启动器级别将所有目标设置为从 iSCSI 启动器接收相同的 CHAP 名称和密钥。默认情况下，所有发现地址或静态目标都继承在启动器级别设置的 CHAP 参数。

前提条件

在设置软件或从属硬件 iSCSI 的 CHAP 参数之前，请先确定是要配置单向 CHAP 还是双向 CHAP。独立硬件 iSCSI 适配器不支持双向 CHAP。

- 在单向 CHAP 中，目标会验证启动器。
- 在双向 CHAP 中，目标和启动器会相互验证。确保对 CHAP 和双向 CHAP 使用不同的密钥。

在配置 CHAP 参数时，确保它们与存储器端的参数相匹配。

CHAP 名称不得超过 511 个字母数字字符，CHAP 密钥不得超过 255 个字母数字字符。有些适配器（例如 QLogic 适配器）的限值更低，CHAP 名称不得超过 255 个字母数字字符，CHAP 密钥不得超过 100 个字母数字字符。

步骤

1 访问“iSCSI 启动器属性”对话框。

2 在**常规**选项卡上，单击 **CHAP**。

3 要配置单向 CHAP，请在 CHAP 下指定以下项：

   a 选择 CHAP 安全级别。

   - **不使用 CHAP，除非目标需要**（仅限软件 iSCSI 和从属硬件 iSCSI）
   - **使用 CHAP，除非已被目标禁止**
   - **使用 CHAP**（仅限软件 iSCSI 和从属硬件 iSCSI）。要能够配置双向 CHAP，必须选择此选项。

   b 指定 CHAP 名称。

   确保指定的名称与在存储器端配置的名称相匹配。

   - 要将 CHAP 名称设置为 iSCSI 启动器名称，请选中**使用启动器名称**。
   - 要将 CHAP 名称设置为除 iSCSI 启动器名称之外的任何其他名称，请取消选中**使用启动器名称**，并在**名称**字段中输入名称。

   c 输入单向 CHAP 密钥以用作身份验证的一部分。确保使用在存储器端输入的相同密钥。

4 要配置双向 CHAP，请先按照步骤 3 中的说明配置单向 CHAP。

   确保为单向 CHAP 选择**使用 CHAP** 选项。然后，在**双向 CHAP** 下，指定以下各项：

   a 选择**使用 CHAP**。

   b 指定双向 CHAP 名称。

   c 输入双向 CHAP 密钥。确保对单向 CHAP 和双向 CHAP 使用不同的密钥。

5 单击**确定**。

6 重新扫描启动器。

如果更改了 CHAP 或双向 CHAP 参数，则它们会用于新的 iSCSI 会话。但对于现有会话，直到注销并重新登录之后才能使用新设置。

设置目标的 CHAP 凭据

对于软件和从属硬件 iSCSI 适配器，可以为每个发现地址或静态目标配置不同的 CHAP 凭据。

在配置 CHAP 参数时，确保它们与存储器端的参数相匹配。CHAP 名称不得超过 511 个字母数字字符，CHAP 密钥不得超过 255 个字母数字字符。

前提条件

在设置软件和从属硬件 iSCSI 的 CHAP 参数之前，请先确定是要配置单向 CHAP 还是双向 CHAP。

- 在单向 CHAP 中，目标会验证启动器。
- 在双向 CHAP 中，目标和启动器会相互验证。确保对 CHAP 和双向 CHAP 使用不同的密钥。

步骤

1 访问“iSCSI 启动器属性”对话框。

2 选择**动态发现**或**静态发现**选项卡。

3 从可用目标的列表中，选择要配置的目标，然后单击**设置 > CHAP**。

4 在 CHAP 区域配置单向 CHAP。

   a 取消选中**从父项继承**。

   b 选择下列选项之一：

   - **不使用 CHAP，除非目标需要**
   - **使用 CHAP，除非已被目标禁止**
   - **使用 CHAP**。要能够配置双向 CHAP，必须选择此选项。

   c 指定 CHAP 名称。

   确保指定的名称与在存储器端配置的名称相匹配。

   - 要将 CHAP 名称设置为 iSCSI 启动器名称，请选中**使用启动器名称**。
   - 要将 CHAP 名称设置为除 iSCSI 启动器名称之外的任何其他名称，请取消选中**使用启动器名称**，并在**名称**字段中输入名称。

   d 输入单向 CHAP 密钥以用作身份验证的一部分。确保使用在存储器端输入的相同密钥。

5 要配置双向 CHAP，请先按照步骤 4 中的说明配置单向 CHAP。

   确保为单向 CHAP 选择**使用 CHAP** 选项。然后，在“双向 CHAP”区域指定以下项：

   a 取消选中**从父项继承**。

   b 选择**使用 CHAP**。

   c 指定双向 CHAP 名称。

   d 输入双向 CHAP 密钥。确保对单向 CHAP 和双向 CHAP 使用不同的密钥。

6 单击**确定**。

7 重新扫描启动器。

如果更改了 CHAP 或双向 CHAP 参数，则它们会用于新的 iSCSI 会话。但对于现有会话，直到注销并重新登录之后才能使用新设置。

禁用 CHAP

如果存储系统不需要 CHAP，则可以将其禁用。

如果在需要 CHAP 身份验证的系统上禁用 CHAP，则现有 iSCSI 会话会保持活动状态，直到重新引导 ESX 主机或者存储系统强制注销为止。在会话结束之后，您将不能再连接需要 CHAP 的目标。

步骤

1 打开“CHAP 凭据”对话框。

2 对于软件和从属硬件 iSCSI 适配器，若要仅禁用双向 CHAP 而保留单向 CHAP，请在“双向 CHAP”区域选择**不使用 CHAP**。

3 要禁用单向 CHAP，请在 CHAP 区域中选择**不使用 CHAP**。

   如果设置了双向 CHAP，则在禁用单向 CHAP 时，双向 CHAP 将自动转换为**不使用 CHAP**。

4 单击**确定**。

配置 iSCSI 的其他参数

可能需要为 iSCSI 启动器配置其他参数。例如，有些 iSCSI 存储系统要求 ARP（地址解析协议）重定向，以在端口间动态移动 iSCSI 流量。在这种情况下，必须在主机上激活 ARP 重定向。

表 8‑2 列出了使用 vSphere Client 可以配置的高级 iSCSI 参数。此外，可以使用 `vicfg-iscsi` vSphere CLI 命令配置部分高级参数。有关信息，请参阅《vSphere 命令行界面安装和脚本指南及 vSphere 命令行界面参考》。

除非在与 VMware 支持团队进行合作，或拥有为设置所提供值的全面信息，否则不要对高级 iSCSI 设置进行任何更改。

表 8‑2 iSCSI 启动器的其他参数

高级参数	描述	配置对象
头摘要	增加数据完整性。启用头摘要后，系统会对每个 iSCSI 协议数据单元 (PDU) 的头部计算校验和，并使用 CRC32C 算法进行验证。	软件 iSCSI 从属硬件 iSCSI
数据摘要	增加数据完整性。启用数据摘要后，系统会对每个 PDU 的数据部分计算校验和，并使用 CRC32C 算法进行验证。 **注意** 使用 Intel Nehalem 处理器的系统会清除软件 iSCSI 的 iSCSI 摘要计算，因此可以减少对性能的影响。	软件 iSCSI 从属硬件 iSCSI
最大未完成 R2T 数	定义在收到确认 PDU 前可转换的 R2T（即将传输）PDU。	软件 iSCSI 从属硬件 iSCSI

表 8–2 iSCSI 启动器的其他参数 （续）

高级参数	描述	配置对象
初次突发长度	指定在执行单个 SCSI 命令期间 iSCSI 启动器可以发送到目标的未经请求的数据的最大数量，以字节为单位。	软件 iSCSI 从属硬件 iSCSI
最大突发长度	传入数据或请求的传出数据 iSCSI 序列中的最大 SCSI 数据负载，以字节为单位。	软件 iSCSI 从属硬件 iSCSI
最大接收数据段长度	在 iSCSI PDU 中可以接收的最大数据段长度，以字节为单位。	软件 iSCSI 独立硬件 iSCSI
会话恢复超时	指定执行会话恢复的时间限制 (秒) 。如果该超时时间超过限值，则 iSCSI 启动器将终止会话。	软件 iSCSI 从属硬件 iSCSI
无操作时间间隔	指定在从 iSCSI 启动器发送到 iSCSI 目标的 NOP-Out 请求之间的时间间隔 (秒) 。NOP-Out 请求充当验证 iSCSI 启动器和 iSCSI 目标之间的连接是否处于活动状态的 ping 机制。	软件 iSCSI 从属硬件 iSCSI
无操作超时	指定主机收到 NOP-In 消息之前的时间限制 (秒) 。该消息由 iSCSI 目标发出，以响应 NOP-Out 请求。无操作超时时间超过限值时，启动器将终止当前会话并启动新的会话。	软件 iSCSI 从属硬件 iSCSI
ARP 重定向	允许存储系统将 iSCSI 流量从一个端口动态移动到另一个端口。ARP 对执行基于阵列的故障切换的存储系统是必需的。	软件和独立硬件 iSCSI (可通过 vSphere CLI 配置)
延迟的 ACK	允许系统对接收的数据包进行延迟确认。	软件 iSCSI 从属硬件 iSCSI

配置 iSCSI 的高级参数

高级 iSCSI 设置控制如标头、数据摘要、ARP 重定向、延迟的 ACK 等参数。通常，不需要更改这些设置，因为 ESX 主机使用分配的预定义值能够正常运行。



小心 除非在与 VMware 支持团队进行合作，或拥有为设置所提供值的全面信息，否则不要对高级 iSCSI 设置进行任何更改。

步骤

1 访问“iSCSI 启动器属性”对话框。

2 要在启动器级别配置高级参数，请在“常规”选项卡上单击**高级**。继续步骤 4。

3 在目标级别配置高级参数。

   在目标级别，只能为软件和从属硬件 iSCSI 适配器配置高级参数。

   a 选择**动态发现**或**静态发现**选项卡。

   b 从可用目标的列表中，选择要配置的目标，然后单击**设置 > 高级**。

4 为要修改的高级参数输入任何所需值，然后单击**确定**保存更改。

数据存储刷新和存储重新扫描操作

数据存储刷新操作可更新 vSphere Client 中显示的数据存储列表和存储信息 (例如数据存储容量) 。执行数据存储管理任务或者在 SAN 配置中进行更改时，可能需要重新扫描存储器。

执行 VMFS 数据存储管理操作时，例如创建 VMFS 数据存储或 RDM、添加数据区和增加或删除 VMFS 数据存储，主机或 vCenter Server 将自动重新扫描和更新存储器。可以通过关闭“主机重新扫描筛选器”来禁用自动重新扫描功能。请参见第 118 页，“关闭 vCenter Server 存储筛选器”。

在某些情况下，需要执行手动重新扫描。可以重新扫描您的主机可用的所有存储器，或者如果使用的是 vCenter Server，则可以重新扫描文件夹、群集和数据中心中的所有主机可用的所有存储器。

如果进行的更改只针对通过特定适配器连接的存储器，则需要重新扫描此适配器。

每次进行以下更改之一后请手动执行重新扫描：

- 在 SAN 上创建新 LUN。
- 更改主机上的路径屏蔽。
- 重新连接线缆。
- 更改 CHAP 设置。
- 在 vCenter Server 中编辑或移除由 vCenter Server 主机和单台主机共享的数据存储之后，向 vCenter Server 中添加该单台主机。

重要事项 如果在某条路径不可用时重新扫描，则主机将从到设备的路径的列表中移除该路径。当该路径再次变得可用并且开始工作时，会立即重新显示在列表中。

执行存储重新扫描

在 SAN 配置中进行更改后，可能需要重新扫描存储器。您可以重新扫描主机可用的所有存储。如果进行的更改只针对通过特定适配器访问的存储器，则只重新扫描此适配器。

如果只需要重新扫描特定主机可用的存储器或通过主机上的特定适配器访问的存储器，请使用此步骤。如果要重新扫描由 vCenter Server 系统管理的所有主机可用的存储，则可以通过右键单击包含这些主机的数据中心、群集或文件夹并选择**重新扫描数据存储**来执行此操作。

步骤

1. 在 vSphere Client 中，选择一台主机，然后单击**配置**选项卡。
2. 在“硬件”面板中，选择**存储适配器**，然后单击“存储适配器”面板上方的**重新扫描**。

   也可右键单击一个适配器，并单击**重新扫描**只对该适配器进行重新扫描。
3. 要发现新的磁盘或 LUN，请选择**扫描新的存储设备**。

   新发现的 LUN 将显示在设备列表上。
4. 要发现新的数据存储或在其配置更改后更新数据存储，请选择**扫描新的 VMFS 卷**。

   发现的新数据存储或 VMFS 卷将出现在数据存储列表上。

创建 VMFS 数据存储

VMFS 数据存储充当虚拟机的存储库。可以在主机发现的基于 SCSI 的任何存储设备上设置 VMFS 数据存储。

前提条件

创建数据存储之前，必须安装和配置存储器所需的全部适配器。重新扫描适配器以发现新增的存储设备。

步骤

1. 登录 vSphere Client，在“清单”面板中选择主机。
2. 单击**配置**选项卡，然后在“硬件”面板中单击**存储器**。
3. 依次单击**数据存储**和**添加存储器**。
4. 选择**磁盘/LUN** 存储器类型，然后单击**下一步**。

5 选择要用于数据存储的设备，然后单击**下一步**。

注意 选择没有在“VMFS 标签”列中显示数据存储名称的设备。如果该名称存在，则设备包含现有 VMFS 数据存储的副本。

如果要格式化的磁盘是空白磁盘，则“当前磁盘布局”页面将自动显示整个磁盘空间，以进行存储器配置。

6 如果磁盘不为空，请在“当前磁盘布局”页面的顶部面板中检查当前磁盘布局，并从底部面板中选择配置选项。

选项	描述
使用所有可用分区	将整个磁盘或 LUN 专门用于单个 VMFS 数据存储。如果选择此选项，则当前在此设备上存储的任何文件系统和数据将被删除。
使用可用空间	在剩余的可用磁盘空间中部署 VMFS 数据存储。

7 单击**下一步**。

8 在属性页面中，输入数据存储名称并单击**下一步**。

9 如果需要，请调整文件系统和容量值。

默认情况下，存储设备上的全部可用空间均可供使用。

10 单击**下一步**。

11 在“即将完成”页面，检查数据存储配置信息，然后单击**完成**。

即会在基于 SCSI 的存储设备上创建数据存储。如果使用 vCenter Server 系统管理主机，则新创建的数据存储会自动添加到所有主机。

网络附加存储

ESX 支持通过 NFS 协议使用 NAS。NFS 协议可以实现 NFS 客户端和 NFS 服务器之间的通信。

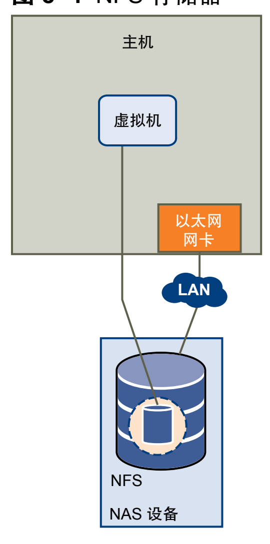
ESX 中内置的 NFS 客户端可让您访问 NFS 服务器并使用 NFS 卷进行存储。ESX 仅支持 TCP 上的 NFS 版本 3。

可使用 vSphere Client 将 NFS 卷配置为数据存储。已配置的 NFS 数据存储会显示在 vSphere Client 中，可将其用来存储虚拟磁盘文件，使用方式与基于 VMFS 的数据存储相同。

注意 ESX 不支持借助于非根凭据启用对 NFS 卷访问权的委派用户功能。

图 8-4 描述了使用 NFS 卷存储其文件的虚拟机。在此配置中，主机连接到 NFS 服务器，此服务器通过常规网络适配器存储虚拟磁盘文件。

图 8–4 NFS 存储器



在基于 NFS 的数据存储上创建的虚拟磁盘采用由 NFS 服务器规定的磁盘格式，通常为精简格式，要求按需分配空间。如果在向该磁盘写入数据时出现虚拟机空间不足的情况，vSphere Client 会通知您需要更多空间。这时您有以下选择：

- 在卷上释放更多空间，以便虚拟机能继续写入磁盘。
- 终止虚拟机会话。终止会话将关闭虚拟机。



小心 当主机访问基于 NFS 的数据存储上的虚拟机磁盘文件时，会在该磁盘文件所驻留的同一目录中生成一个 `.lck-XXX` 锁定文件，以阻止其他主机访问该虚拟磁盘文件。不要移除 `.lck-XXX` 锁定文件，因为如果没有该文件，正在运行的虚拟机将无法访问其虚拟磁盘文件。

作为常用文件的存储库的 NFS 数据存储

除了在 NFS 数据存储上存储虚拟磁盘以外，还可以使用 NFS 作为 ISO 映像、虚拟机模板等的中央存储库。

若要将 NFS 用作共享存储库，可以在 NFS 服务器上创建目录，然后在所有主机上将它作为数据存储挂载。如果使用 ISO 映像的数据存储，可以将虚拟机的 CD-ROM 设备连接到数据存储上的 ISO 文件，并从 ISO 文件安装客户机操作系统。

注意 如果存储文件的基础 NFS 卷是只读的，则应确保该卷由 NFS 服务器导出为只读共享，或在 ESX 主机上将它配置为只读数据存储。否则，主机会认为该数据存储可以读写，并可能无法打开文件。

创建基于 NFS 的数据存储

可以使用添加存储器向导挂载 NFS 卷并将其用作 VMFS 数据存储。

前提条件

因为 NFS 需要网络连接来访问存储在远程服务器上的数据，因此在配置 NFS 之前，必须首先配置 VMkernel 网络。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。
2 单击**配置**选项卡，然后在“硬件”面板中单击**存储器**。
3 依次单击**数据存储**和**添加存储器**。
4 选择**网络文件系统**作为存储器类型，然后单击**下一步**。

5 输入服务器名称、挂载点文件夹名称以及数据存储名称。

注意 当在不同主机上挂载相同 NFS 卷时，确保各主机之间的服务器名称和文件夹名称相同。如果名称不完全匹配，例如，如果您在一台主机上输入 `share` 作为文件夹名称，而在另一台主机上使用 `/share` 作为文件夹名称，则主机会将同一 NFS 卷视为两个不同的数据存储。这可能导致诸如 vMotion 之类的功能失效。

6 （可选）如果 NFS 服务器将卷作为只读导出，则选择**挂载只读 NFS**。

7 单击**下一步**。

8 在“网络文件系统摘要”页面中，检查配置选项，然后单击**完成**。

创建诊断分区

要成功运行，主机必须具有用于存储核心转储的诊断分区或转储分区来提供调试和技术支持持。可在本地磁盘、专用 SAN LUN 或共享 SAN LUN 上创建诊断分区。

诊断分区不能位于通过软件 iSCSI 启动器访问的 iSCSI LUN 上。

每台主机均必须拥有一个 100MB 的诊断分区。如果多台主机共享一个 SAN，请为每台主机配置一个 100MB 大小的诊断分区。



小心 如果两个共享诊断分区的主机出现故障，并将核心转储保存到相同插槽，则核心转储可能丢失。若要收集核心转储数据，在主机出现故障之后，请立即重新引导主机，并提取日志文件。但是，在收集第一个主机的诊断数据之前，如果另一个主机出现故障，第二个主机将无法保存核心转储。

如果使用的是 ESX 主机，通常在安装 ESX 时，通过选择**建议的分区**来创建诊断分区。安装程序将自动为主机创建诊断分区。如果选择**高级分区**并选择在安装期间不指定诊断分区，则可以使用添加存储器向导配置诊断分区。

创建诊断分区

可以为主机创建诊断分区。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 单击**配置**选项卡，然后在“硬件”面板中单击**存储器**。

3 依次单击**数据存储**和**添加存储器**。

4 选择**诊断**并单击**下一步**。

如果看不到**诊断**选项，则表示主机已拥有诊断分区。

可使用 vSphere CLI 上的 `vicfg-dumppart -l` 命令查询和扫描主机的诊断分区。

5 指定诊断分区的类型。

选项	描述
本地专用存储器	在本地磁盘上创建诊断分区。此分区将仅存储主机的故障信息。
SAN 专用存储器	在非共享 SAN LUN 上创建诊断分区。此分区将仅存储主机的故障信息。
SAN 共享存储器	在共享 SAN LUN 上创建诊断分区。此分区将由多个主机访问并且可以存储多个主机的故障信息。

6 单击**下一步**。

7 选择要用于诊断分区的设备，然后单击**下一步**。

8 检查分区配置信息，然后单击**完成**。

管理存储器 9

在创建数据存储之后，可以更改其属性，使用文件夹根据业务需求对数据存储进行分组，或删除未使用的数据存储。也可能需要为存储器设置多路径或对数据存储副本进行再签名。

本章讨论了以下主题：

管理数据存储

ESX 系统使用数据存储来存储与其虚拟机关联的所有文件。在创建数据存储之后，可以通过执行多个任务对其进行管理。

数据存储是一个逻辑存储单元，它可以使用一个物理设备、一个磁盘分区或若干个物理设备上的磁盘空间。数据存储可以存在于不同类型的物理设备（包括 SCSI、iSCSI、光纤通道 SAN 或 NFS）上。

可使用以下方式之一将数据存储添加到 vSphere Client 中：

- 当主机添加到清单时发现。vSphere Client 显示能够由主机识别的任何数据存储。
- 使用**添加存储器**命令在可用存储设备上创建。

创建数据存储之后，可以使用它们来存储虚拟机文件。通过重命名、移除和设置访问控制权限，可以对其进行管理。此外，可以对数据存储进行分组以便于组织，以及一次对多个组设置相同权限。

有关设置数据存储的访问控制权限的信息，请参见 vSphere Client 帮助。

重命名数据存储

可更改现有数据存储的名称。

步骤

1 显示数据存储。

2 右键单击要重命名的数据存储，然后选择**重命名**。

3 键入新的数据存储名称。

如果使用 vCenter Server 系统管理主机，则新名称将显示在所有可访问数据存储的主机上。

为数据存储分组

如果您使用 vCenter Server 系统管理主机，则可以将数据存储分组到文件夹中。这允许您根据业务实践组织数据存储，并对组中的数据存储一次性分配相同权限和警报。

步骤

1 登录 vSphere Client。

2 如有必要，创建数据存储。

  有关详细信息，请参见 vSphere Client 帮助。

3 在”清单“面板中，选择**数据存储**。

4 选择包含要分组的数据存储的数据中心。

5 在快捷方式菜单中，单击**新建文件夹**图标。

6 为该文件夹提供一个描述性名称。

7 单击各个数据存储，然后将其拖动到该文件夹中。

删除数据存储

可以删除任何类型的 VMFS 数据存储（包括已挂载但未再签名的副本）。删除数据存储时，会对其造成损坏，而且它将从具有数据存储访问权限的所有主机中消失。

前提条件

在删除数据存储之前，从数据存储中移除所有虚拟机。确保没有任何其他主机正在访问该数据存储。

步骤

1 显示数据存储。

2 右键单击要删除的数据存储并单击**删除**。

3 确认要删除数据存储。

卸载数据存储

卸载数据存储时，它会保持原样，但是在指定的主机上再也看不到该存储。它继续出现在其他主机上并在这些主机上它保持挂载状态。

只能卸载以下类型的数据存储：

- NFS 数据存储
- 已挂载却没有再签名的 VMFS 数据存储副本

不能卸载活动的已挂载数据存储。

步骤

1 显示数据存储。

2 右键单击要卸载的数据存储，然后选择**卸载**。

3 如果数据存储已共享，请指定不应再访问该数据存储的主机。

   a 如果需要，请取消选中要使其中的数据存储保持挂载状态的主机。

      默认情况下，会选中所有主机。

   b 单击**下一步**。

   c 检查要从中卸载数据存储的主机列表，然后单击**完成**。

4 确认要卸载数据存储。

更改 VMFS 数据存储属性

创建基于 VMFS 的数据存储以后，可以进行修改。例如，如果您需要更多空间，则可以增加数据存储容量。如果有 VMFS-2 数据存储，可将其升级到 VMFS-3 格式。

使用 VMFS 格式的数据存储部署在基于 SCSI 的存储设备上。

无法重新格式化远程主机正在使用的 VMFS 数据存储。如果尝试这样做，则会出现一条警告，该警告会指出正在使用的数据存储的名称和正在使用该数据存储的主机的名称。此警告也会出现在 VMkernel 和 VMkwarning 日志文件中。

根据 vSphere Client 是连接到 vCenter Server 系统还是直接连接到主机，“数据存储属性”对话框的访问方式会有所不同。

- 仅适用于 vCenter Server。要访问“数据存储属性”对话框，请从清单中选择数据存储，单击**配置**选项卡，然后单击**属性**。
- vCenter Server 和 ESX 主机。要访问“数据存储属性”对话框，请从清单中选择主机，单击**配置**选项卡，然后单击**存储器**。从“数据存储”视图中，选择要修改的数据存储，然后单击**属性**。

增加 VMFS 数据存储

需要在数据存储上创建新虚拟机时，或者此数据存储上运行的虚拟机需要更多空间时，可以动态增加 VMFS 数据存储的容量。

使用下列方法之一：

- 添加新数据区。数据区是存储设备或 LUN 上的分区。最多可以将相同类存储型的 32 个新数据区添加到现有 VMFS 数据存储。跨区的 VMFS 数据存储可以随时使用其所有任意数据区。使用下一个数据区之前，不需要填满特定数据区。
- 在现有 VMFS 数据存储中增加数据区，以便它填满可用的相邻容量。只有紧随其后就有可用空间的数据区才是可扩展的。

注意 如果共享数据存储有启动的虚拟机并被 100% 占用，则仅可以从注册了已启动虚拟机的主机增加数据存储的容量。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 单击**配置**选项卡，然后单击**存储器**。

3 从“数据存储”视图中，选择要增加的数据存储，然后单击**属性**。

4 单击**增加**。

5 从存储设备列表中选择设备，然后单击**下一步**。

   - 如果要添加新数据区，请选择“可扩展的”列显示为“否”的设备。
   - 如果要展开现有数据区，请选择“可扩展的”列显示为“是”的设备。

6 从底部面板选择配置选项。

根据磁盘的当前布局和以前的选择，您看到的选项可能有所不同。

选项	描述
使用可用空间添加新数据区	在该磁盘上增加可用空间作为新的数据存储数据区。
使用可用空间扩展现有数据区	将现有数据区增加到所需容量。
使用可用空间	在剩余的可用磁盘空间中部署数据区。此选项仅在添加数据区时可用。
使用所有可用分区	将整个磁盘专用于单个数据存储数据区。此选项仅在添加数据区并且所格式化的磁盘非空白时可用。磁盘将被重新格式化，其中所包含的数据存储和任何数据将被擦除。

7 设置数据区的容量。

默认情况下，存储设备上的全部可用空间均可供使用。

8 单击**下一步**。

9 检查推荐的数据区布局和数据存储的新配置，然后单击**完成**。

下一步

在增加了共享 VMFS 数据存储中的数据区之后，在可以访问此数据存储的每个主机上刷新数据存储，以便 vSphere Client 可以显示所有主机的正确数据存储容量。

升级数据存储

ESX 包括 VMFS 第 3 版 (VMFS-3)。如果数据存储使用 VMFS-2 格式化，则可以读取以 VMFS-2 格式存储的文件，但不能对其进行写入。要拥有对文件的完整访问权限，请将 VMFS-2 升级为 VMFS-3。

将 VMFS-2 升级为 VMFS-3 时，ESX 文件锁定机制可确保无远程主机或本地进程访问转换中的 VMFS 数据存储。主机保留数据存储上的所有文件。

使用升级选项之前，请考虑以下注意事项：

- 提交或放弃对要升级的 VMFS-2 卷中虚拟磁盘的任何更改。
- 备份 VMFS-2 卷。
- 确保没有已启动的虚拟机在使用此 VMFS-2 卷。
- 确保无其他 ESX 主机在访问此 VMFS-2 卷。

VMFS-2 至 VMFS-3 的转换是一种单向过程。将基于 VMFS 的数据存储转换成 VMFS-3 后，不能将其恢复为 VMFS-2。

要升级 VMFS-2 文件系统，其文件块大小不得超过 8 MB。

步骤

1 登录 vSphere Client，在“清单”面板中选择主机。

2 单击**配置**选项卡，然后单击**存储器**。

3 选择一个使用 VMFS-2 格式的数据存储。

4 单击**升级到 VMFS-3**。

5 在可以看到数据存储的所有主机上执行重新扫描。

管理重复 VMFS 数据存储

当 LUN 包含 VMFS 数据存储副本时，您可以使用现有签名或通过分配新签名来挂载该数据存储。

在 LUN 中创建的每个 VMFS 数据存储都有一个唯一的 UUID，该 UUID 存储在文件系统超级块中。对 LUN 进行复制或生成快照后，生成的 LUN 副本的每个字节都与原始 LUN 完全相同。因此，如果原始 LUN 包含具有 UUID X 的 VMFS 数据存储，则 LUN 副本会显示包含具有完全相同 UUID X 的相同的 VMFS 数据存储或 VMFS 数据存储副本。

ESX 可以确定 LUN 是否包含 VMFS 数据存储副本，并使用其原始 UUID 挂载数据存储副本，或更改 UUID 从而对该数据存储进行再签名。

使用现有签名挂载 VMFS 数据存储

可能无需再签名 VMFS 数据存储副本。可以挂载 VMFS 数据存储副本，而不更改其签名。

例如，作为灾难恢复计划的一部分，可以在辅助站点上维护虚拟机的同步副本。在主站点发生灾难时，可以在辅助站点上挂载数据存储副本并启动虚拟机。

重要事项 仅当与具有相同 UUID 的原始 VMFS 数据存储不冲突时，才可以挂载 VMFS 数据存储副本。要挂载该副本，原始 VMFS 数据存储必须处于脱机状态。

挂载 VMFS 数据存储时，ESX 允许对驻留在 LUN 副本上的数据存储执行读取和写入操作。LUN 副本必须为可写入状态。在系统重新引导后，数据存储挂载也是持久有效的。

由于 ESX 不允许对挂载的数据存储进行再签名，所以请在进行再签名之前卸载数据存储。

使用现有签名挂载 VMFS 数据存储

如果不需要对 VMFS 数据存储副本进行再签名，则无需更改其签名即可挂载。

前提条件

在挂载 VMFS 数据存储之前，请在主机上执行存储重新扫描，以便更新为其显示的 LUN 视图。

步骤

1 登录 vSphere Client，然后在“清单”面板中选择服务器。

2 单击**配置**选项卡，然后在“硬件”面板中单击**存储器**。

3 单击**添加存储器**。

4 选择**磁盘/LUN** 存储器类型，然后单击**下一步**。

5 从 LUN 列表中，选择数据存储名称显示在“VMFS 标签”列中的 LUN，然后单击**下一步**。

  “VMFS 标签”列中显示的名称表示 LUN 包含现有 VMFS 数据存储的副本。

6 在“挂载选项”下面，选择**保留现有的签名**。

7 在“即将完成”页面，检查数据存储配置信息，然后单击**完成**。

下一步

如果稍后要对挂载的数据存储进行再签名，则必须先将其卸载。

对 VMFS 副本进行再签名

使用数据存储再签名保留 VMFS 数据存储副本上所存储的数据。对 VMFS 副本进行再签名时，ESX 会为副本分配新的 UUID 和新的标签，并将副本挂载为与原始数据存储明显不同的数据存储。

分配到数据存储的新标签的默认格式是 `snap-`*`snapID`*`-`*`oldLabel`*，其中 *snapID* 是整数并且 *oldLabel* 是原始数据存储的标签。

在执行数据存储再签名时，请考虑以下几点：

- 数据存储再签名不可逆。
- 不再将包含再签名的 VMFS 数据存储的 LUN 副本视为 LUN 副本。
- 仅当跨区数据存储的所有数据区联机时，才可对其进行再签名。
- 再签名过程是应急过程，并具有容错性。如果过程中断，可以稍后恢复。
- 可以挂载新的 VMFS 数据存储，而无需承担其 UUID 与其他任何数据存储 UUID 相冲突的风险，如 LUN 快照层次结构中的祖先或子项。

对 VMFS 数据存储副本进行再签名

如果要保留 VMFS 数据存储副本上所存储的数据，请使用数据存储再签名。

前提条件

要对挂载的数据存储副本进行再签名，请先将其卸载。

对 VMFS 数据存储进行再签名之前，请在主机上执行存储重新扫描，以便主机更新为其显示的 LUN 视图并发现所有 LUN 副本。

步骤

1 登录 vSphere Client，然后在“清单”面板中选择服务器。
2 单击**配置**选项卡，然后在“硬件”面板中单击**存储器**。
3 单击**添加存储器**。
4 选择**磁盘/LUN** 存储器类型，然后单击**下一步**。
5 从 LUN 列表中，选择数据存储名称显示在“VMFS 标签”列中的 LUN，然后单击**下一步**。

  “VMFS 标签”列中显示的名称表示 LUN 包含现有 VMFS 数据存储的副本。
6 在“挂载选项”下，选择**分配新签名**，并单击**下一步**。
7 在“即将完成”页面，检查数据存储配置信息，然后单击**完成**。

下一步

进行再签名之后，可能需要执行以下操作：

- 如果再签名的数据存储包含虚拟机，则在虚拟机文件中更新对原始 VMFS 数据存储的引用，这些虚拟机文件包括 `.vmx`、`.vmdk`、`.vmsd` 和 `.vmsn`。
- 要启动虚拟机，请在 vCenter Server 中注册它们。

在 ESX 中使用多路径

要维护 ESX 主机及其存储器之间的持续连接，ESX 必须支持多路径。通过多路径技术，可以使用多个物理路径，这些路径在 ESX 主机和外部存储设备之间传输数据。

如果 SAN 网络中的某个元件（如 HBA、交换机或电缆）出现故障，ESX 可以使用备用物理路径访问存储设备。此过程称为路径故障切换。除了路径故障切换以外，多路径还提供负载平衡，它在多路径之间重新分配 I/O 负载，以减少或免除潜在的瓶颈。

管理多路径

为管理存储多路径，ESX 使用特殊的 VMkernel 层（即，可插入存储架构 (PSA)）。PSA 是一个开放式模块框架，用于协调多个多路径插件 (MPP) 的同时操作。

ESX 默认情况下提供的 VMkernel 多路径插件是 VMware 本机多路径插件 (NMP)。NMP 是管理子插件的可扩展模块。NMP 子插件有两种类型，即存储阵列类型插件 (SATP) 和路径选择插件 (PSP)。SATP 和 PSP 可以是 VMware 提供的内置插件，也可以由第三方提供。

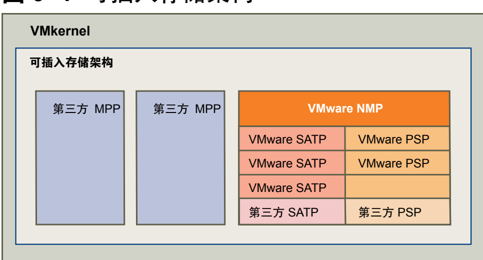
如果需要更多多路径功能，第三方还可以提供 MPP 以作为默认 NMP 的附属或替代运行。

当协调 VMware NMP 和所安装的任何第三方 MPP 时，PSA 将执行以下任务：

- 加载和卸载多路径插件。
- 对特定插件隐藏虚拟机细节。
- 将特定逻辑设备的 I/O 请求路由到管理该设备的 MPP。
- 处理逻辑设备的 I/O 排队操作。
- 在虚拟机之间实现逻辑设备带宽共享。
- 处理物理存储 HBA 的 I/O 排队操作。
- 处理物理路径发现和移除。
- 提供逻辑设备和物理路径 I/O 统计信息。

如图 9-1 所示，多个第三方 MPP 可以与 VMware NMP 并行运行。安装后，第三方 MPP 将替代 NMP 的行为，并且完全控制指定存储设备的路径故障切换和负载平衡操作。

图 9-1 可插入存储架构



多路径模块执行以下操作：

- 管理物理路径声明和取消声明。
- 管理逻辑设备的创建、注册和取消注册。
- 将物理路径与逻辑设备关联。
- 支持路径故障检测和修复。

- 处理逻辑设备的 I/O 请求：
  - 为请求选择最佳物理路径。
  - 根据存储设备，执行处理路径故障和 I/O 命令重试所需的特定操作。
- 支持管理任务，如中止或重置逻辑设备。

VMware 多路径模块

默认情况下，ESX 提供名为本机多路径插件 (NMP) 的可扩展多路径模块。

一般来说，VMware NMP 支持 VMware 存储 HCL 上列出的所有存储阵列，并基于阵列类型提供默认的路径选择算法。还将一组物理路径与特定存储设备或 LUN 关联。存储阵列类型插件 (SATP) 负责处理给定存储阵列的路径故障切换。路径选择插件 (PSP) 负责确定哪个物理路径用于向存储设备发出 I/O 请求。SATP 和 PSP 是 NMP 模块中的子插件。

安装 ESX 时，会自动安装适合所用阵列的 SATP。您不需要获取或下载任何 SATP。

VMware SATP

存储阵列类型插件 (SATP) 与 VMware NMP 一起运行，负责特定于阵列的操作。

ESX 为 VMware 支持的各种类型阵列提供 SATP。它还提供默认 SATP 以支持非特定的主动-主动和 ALUA 存储阵列，以及适用于直接连接的设备的本地 SATP。每个 SATP 适合特定类别的存储阵列的特殊特性，并可以执行检测路径状况和激活被动路径所需的特定于阵列的操作。因此，NMP 模块本身可以使用多个存储阵列，而无需了解存储设备的特性。

在 NMP 确定要为特定存储设备使用哪个 SATP 并将该 SATP 与存储设备的物理路径相关联之后，该 SATP 会执行以下任务：

- 监控每个物理路径的健康状况。
- 报告每个物理路径的状况变化。
- 执行存储器故障切换所需的特定于阵列的操作。例如，对于主动-被动设备，它可以激活被动路径。

VMware PSP

路径选择插件 (PSP) 与 VMware NMP 一起运行，负责选择 I/O 请求的物理路径。

VMware NMP 根据与每个逻辑设备物理路径关联的 SATP 为该设备分配默认 PSP。可以替代默认 PSP。

默认情况下，VMware NMP 支持以下 PSP：

最近使用 (VMW_PSP_MRU)
选择 ESX 主机最近用于访问指定设备的路径。如果此路径不可用，则主机会切换到替代路径并在该新路径可用时继续使用它。MRU 是主动-被动阵列的默认路径策略。

固定 (VMW_PSP_FIXED)
使用指定首选路径（如果已配置）。否则，它将使用在系统引导时间发现的第一个工作路径。如果主机不能使用首选路径，则它会选择随机替代可用路径。一旦首选路径可用，主机便会恢复到首选路径。“固定”是主动-主动阵列的默认路径策略。



小心　如果用于主动-被动阵列，则**固定**路径策略可能会导致路径抖动。

VMW_PSP_FIXED_AP
将“固定”功能扩展到主动-被动阵列和 ALUA 模式阵列。

循环 (VMW_PSP_RR)
使用路径选择算法轮流选择所有可用的活动路径，并在路径之间启用负载平衡。

VMware NMP I/O 流

当虚拟机向 NMP 管理的存储设备发出 I/O 请求时，将发生以下过程。

1 NMP 调用分配给此存储设备的 PSP。

2 PSP 将选择要通过其发出 I/O 的相应物理路径。

3 NMP 在 PSP 选择的路径上发出 I/O 请求。

4 如果 I/O 操作成功，则 NMP 报告其完成。

5 如果 I/O 操作报告错误，则 NMP 调用适当的 SATP。

6 SATP 解释 I/O 命令错误，并在适当时激活非活动路径。

7 此时将调用 PSP 以选择要通过其发出 I/O 的新路径。

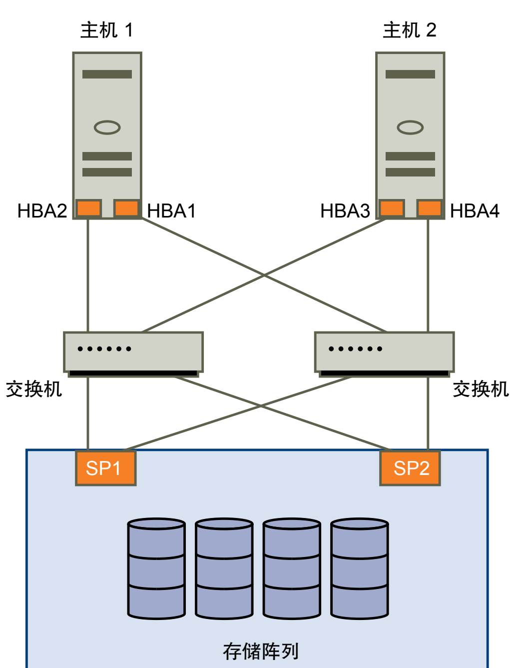
本地存储器和光纤通道 SAN 中的多路径

在简单的多路径本地存储器拓扑中，可以使用一台具有两个 HBA 的 ESX 主机。ESX 主机通过两根电缆连接到双端口本地存储系统。使用这种配置时，如果 ESX 主机和本地存储系统之间的某个连接元素发生故障，可以确保实现容错。

为了支持 FC SAN 中的路径切换，ESX 主机通常具有两个或更多个可用的 HBA，使用一个或多个交换机可以从这些 HBA 访问存储阵列。或者，该设置可以包括一个 HBA 和两个存储处理器，以便 HBA 可以使用其他路径访问磁盘阵列。

在图 9-2 中，多条路径将每台服务器与存储设备相连。例如，如果 HBA1 或 HBA1 与交换机之间的链路发生故障，HBA2 会取代 HBA1 并提供服务器和交换机之间的连接。一个 HBA 取代另一个 HBA 的过程称为 HBA 故障切换。

图 9–2 光纤通道多路径



同样，如果 SP1 或 SP1 与交换机之间的链路中断，SP2 会取代 SP1 并提供交换机和存储设备之间的连接。此过程称为 SP 故障切换。ESX 通过多路径功能支持 HBA 和 SP 故障切换。

iSCSI SAN 中的多路径

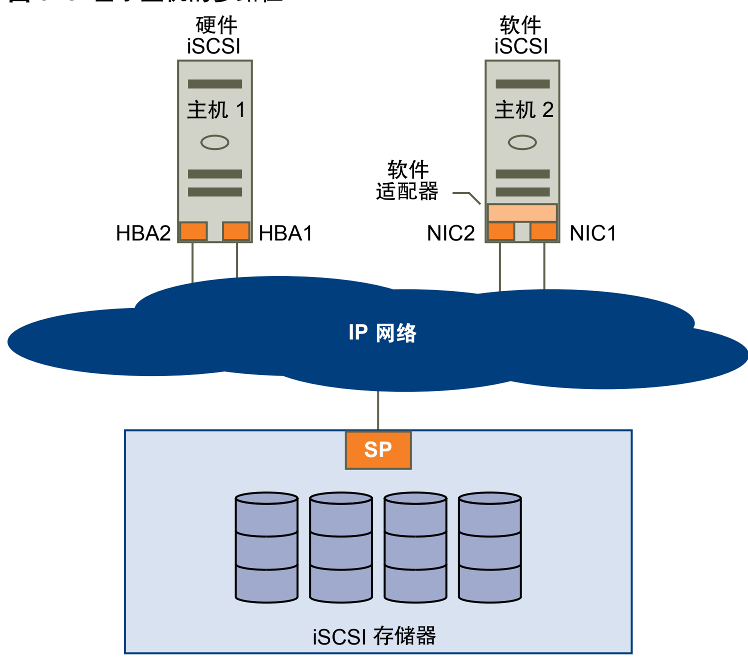
在 iSCSI 存储器中，您可以利用 IP 网络提供的多路径支持。此外，对于所有类型的 iSCSI 启动器，ESX 支持基于主机的多路径。

ESX 可以使用 IP 网络中内置的多路径支持，该支持允许网络执行路由操作。通过动态发现，iSCSI 启动器获得目标地址列表，启动器可以使用这些地址作为通往 iSCSI LUN 的多条路径来实现故障切换目的。

ESX 还可支持基于主机的多路径。

图 9-3 显示了对于不同类型的 iSCSI 启动器可能的多路径设置。

图 9-3 基于主机的多路径



硬件 iSCSI 中的多路径

在硬件 iSCSI 中，主机通常具有两个或更多的可用硬件 iSCSI 适配器，使用一个或多个交换机可从这些适配器到达存储系统。或者，设置可能包括一个适配器和两个存储处理器，以便适配器可以使用不同的路径到达存储系统。

如图 9-3 所示，主机 1 有两个硬件 iSCSI 适配器（HBA1 和 HBA2），用于提供两条到存储系统的物理路径。主机上的多路径插件，不论是 VMkernel NMP 还是任何第三方 MPP，默认情况下都可以访问这些路径，并可以监控每个物理路径的健康状况。例如，如果 HBA1 或 HBA1 与网络之间的链路发生故障，多路径插件可以将路径切换到 HBA2。

软件 iSCSI 的多路径

如图 9-3 的主机 2 所示，通过软件 iSCSI，您可以使用多张网卡为主机和存储系统间的 iSCSI 连接提供故障切换和负载平衡功能。

对于此设置，由于多路径插件没有主机上物理网卡的直接访问权，因此，您必须将每个物理网卡连接到单独的 VMkernel 端口，然后使用端口绑定技术将所有的 VMkernel 端口与软件 iSCSI 启动器相关联。因此，连接到单独网卡的每个 VMkernel 端口将成为 iSCSI 存储堆栈及其存储感知多路径插件可使用的另一条路径。

有关如何为软件 iSCSI 配置多路径的详细信息，请参见第 64 页，“软件 iSCSI 和从属硬件 iSCSI 的网络配置”。

路径扫描和声明

启动 ESX 主机或重新扫描存储适配器时，主机会发现它可以使用的存储设备的所有物理路径。根据 `/etc/vmware/esx.conf` 文件中所定义的一组声明规则，主机会确定应声明特定设备路径并负责管理该设备的多路径支持的多路径插件 (MPP)。

默认情况下，主机每 5 分钟执行一次定期路径评估，从而促使相应 MPP 声明任何尚未声明的路径。

对声明规则进行了编号。对于每个物理路径，主机都通过声明规则运行，首先从最小编号开始。然后，会将物理路径的属性与声明规则中的路径规范进行比较。如果二者匹配，主机会分配声明规则中指定的一个 MPP 来管理物理路径。此过程将持续到所有物理路径均由相应 MPP（第三方多路径插件或本机多路径插件 (NMP)）声明后才结束。

有关多路径插件的一般信息，请参见第 109 页，“管理多路径”。

对于由 NMP 模块管理的路径，将应用第二组声明规则。这些规则确定哪些存储阵列类型插件 (SATP) 应当用于管理特定阵列类型的路径，以及哪些路径选择插件 (PSP) 用于各个存储设备。例如，对于属于 EMC CLARiiON CX 存储系列并且未配置为 ALUA 设备的存储设备，默认 SATP 是 VMW_SATP_CX，默认 PSP 是“最近使用”。

使用 vSphere Client 查看主机用于特定存储设备的 SATP 和 PSP，以及该存储设备的所有可用路径的状态。如果需要，可以使用 vSphere Client 更改默认 VMware PSP。要更改默认 SATP，需要使用 vSphere CLI 修改声明规则。

有关可用于管理 PSA 的命令的详细说明，请参见《vSphere 命令行界面安装和脚本指南》以及《vSphere 命令行界面参考》。

查看路径信息

使用 vSphere Client 确定 ESX 主机用于特定存储设备的 SATP 和 PSP，以及该存储设备的所有可用路径的状态。可以从“数据存储”和“设备”视图访问路径信息。对于数据存储，请检查与部署了数据存储的设备相连的路径。

路径信息包括分配用来管理设备的 SATP、路径选择策略 (PSP)、路径及其物理特性的列表（如适配器和各条路径使用的目标）以及各条路径的状态。其中会显示以下路径状态信息：

活动
可用于对 LUN 发出 I/O 的路径。目前用于传输数据的单个或多个工作路径标记为“活动”(I/O)。

> **注意** 对于运行 ESX 3.5 或更低版本的主机，术语“主动”意为只有一条路径被主机用来向 LUN 发出 I/O。

备用
路径处于工作状态，并且在活动路径发生故障时可用于 I/O。

已禁用
路径已禁用，无法传输数据。

失效
软件无法通过此路径连接磁盘。

如果正在使用**固定**路径策略，就可以看到哪一条路径是首选路径。首选路径的“首选”列标有一个星号 (*)。

查看数据存储路径

使用 vSphere Client 检查连接到部署了数据存储的存储设备的路径。

步骤

1 登录 vSphere Client，在“清单”面板中选择服务器。

2 单击**配置**选项卡，然后在“硬件”面板中单击**存储器**。

3 在“查看”下方单击**数据存储**。

4 在已配置的数据存储列表中，选择要查看或配置其路径的数据存储。

“详细信息”面板显示用来访问设备的路径总数，以及是否有任何路径已中断或已禁用。

5 单击**属性 > 管理路径**以打开“管理路径”对话框。

可以使用“管理路径”对话框来启用或禁用路径、设置多路径策略，以及指定首选路径。

查看存储设备路径

使用 vSphere Client 查看主机用于特定存储设备的 SATP 和 PSP，以及该存储设备的所有可用路径的状态。

步骤

1 登录 vSphere Client，在“清单”面板中选择服务器。

2 单击**配置**选项卡，然后在“硬件”面板中单击**存储器**。

3 在“查看”下方单击**设备**。

4 单击**管理路径**以打开“管理路径”对话框。

设置路径选择策略

对于每个存储设备，ESX 主机都将根据 `/etc/vmware/esx.conf` 文件中所定义的声明规则来设置路径选择策略。

默认情况下，VMware 支持以下路径选择策略。如果在主机上安装了第三方的 PSP，其策略也将显示于列表中。

固定 (VMW_PSP_FIXED)
当通往磁盘的首选路径可用时，主机将始终使用此路径。如果主机无法通过首选路径访问磁盘，它会尝试替代路径。“固定的”是主动-主动存储设备的默认策略。

固定的 AP (VMW_PSP_FIXED_AP)
将“固定”功能扩展到主动-被动阵列和 ALUA 模式阵列。

最近使用 (VMW_PSP_MRU)
主机选择它最近使用的路径。当路径不可用时，主机会选择一个替代路径。当该路径再次可用时，主机不会恢复到原始路径。没有 MRU 策略的首选路径设置。MRU 是主动-被动存储设备的默认策略。

循环 (VMW_PSP_RR)
当连接到主动-被动阵列时，主机使用自动路径选择算法轮流选择所有活动路径；或者，当连接到主动-主动阵列时，主机使用该算法轮流选择所有可用路径。这样可在主机可用的物理路径之间实现负载平衡。

负载平衡是在路径之间分配 I/O 请求的过程。目的是针对吞吐量（例如每秒 I/O 流量、每秒兆字节数或响应时间）实现最佳性能。

表 9‑1 总结了主机的行为随不同阵列类型和故障切换策略变化的情况。

表 9‑1 路径策略影响

策略/控制器	主动/主动	主动/被动
最近使用	发生路径故障后进行故障恢复需要管理员操作。	发生路径故障后进行故障恢复需要管理员操作。
固定的	连接恢复后，VMkernel 继续使用首选路径。	VMkernel 尝试继续使用首选路径。这会导致路径抖动或故障，因为另一 SP 现拥有 LUN 的所有权。
循环	无故障恢复。	选择了循环调度中的下一路径。
固定的 AP	对于 ALUA 阵列，VMkernel 选择设置为首选路径的路径。 对于 A/A 和 A/P 以及 ALUA 阵列，只有在路径抖动避免算法允许故障恢复时，VMkernel 才继续使用首选路径。	

更改路径选择策略

通常，不需要更改主机用于特定存储设备的默认多路径设置。但是，如果要进行任何更改，可以使用“管理路径”对话框修改路径选择策略并指定“固定”策略的首选路径。

步骤

1 从“数据存储”视图或“设备”视图打开“管理路径”对话框。

2 选择路径选择策略。

   默认情况下，VMware 支持以下路径选择策略。如果在主机上安装了第三方的 PSP，其策略也将显示于列表中。

   - **固定 (VMW_PSP_FIXED)**
   - **固定的 AP (VMW_PSP_FIXED_AP)**
   - **最近使用 (VMW_PSP_MRU)**
   - **循环 (VMW_PSP_RR)**

3 对于“固定”策略，请指定首选路径，方法是：右键单击要作为首选路径分配的路径并选择**首选**。

4 单击**确定**以保存设置并退出对话框。

禁用路径

由于维护或其他原因，可以暂时禁用路径。您可以使用 vSphere Client 完成此操作。

步骤

1 从“数据存储”视图或“设备”视图打开“管理路径”对话框。

2 在“路径”面板中，右键单击要禁用的路径，然后选择**禁用**。

3 单击**确定**以保存设置并退出对话框。

还可以通过右键单击列表中的路径，然后选择**禁用**来从适配器的“路径”视图禁用路径。

存储硬件加速

硬件加速功能使主机能够将特定虚拟机和存储管理操作卸载到合规存储硬件。利用存储硬件的辅助，主机可以更快地执行这些操作并且占用更少的 CPU、内存和存储结构带宽。

为实现硬件加速功能，可插入存储架构 (PSA) 结合使用特殊阵列集成插件（称为 VAAI 插件）以及一个阵列集成筛选器（称为 VAAI）。PSA 可自动将 VAAI 筛选器和供应商特定的 VAAI 插件附加到这些支持硬件加速的存储设备。

要查看和管理主机上可用的 VAAI 筛选器和 VAAI 插件，请使用 vSphere CLI 命令。

有关这些命令的说明，请参见《vSphere 命令行界面安装和脚本指南》和《vSphere 命令行界面参考》。

硬件加速要求和优点

仅当结合使用相应的主机和存储阵列时，硬件加速功能才起作用。

使用下列主机和存储阵列：

- ESX 版本 4.1 或更高版本。
- 支持基于存储的硬件加速的存储阵列。ESX 版本 4.1 不支持对 NAS 存储设备使用硬件加速。

在主机上，硬件加速功能在默认情况下已启用。要在存储器端启用硬件加速，请咨询存储器供应商。某些存储阵列要求在存储器端明确激活硬件加速支持。

当支持硬件加速功能时，主机在硬件方面可以有所改善，从而可以更快和更有效地执行下列操作：

- 通过 Storage vMotion 迁移虚拟机
- 从模板中部署虚拟机
- 克隆虚拟机或模板
- 虚拟机文件的 VMFS 群集锁定和元数据操作
- 写入精简置备的虚拟磁盘和厚虚拟磁盘
- 创建容错虚拟机

硬件加速支持状态

对于每个存储设备和数据存储，vSphere Client 会在“设备”视图和“数据存储”视图的“硬件加速”列中显示硬件加速支持状态。

状态值为“未知”、“支持”和“不支持”。初始值为“未知”。在主机成功执行卸载操作后，状态将更改为“支持”。如果卸载操作失败，状态将更改为“不支持”。

当存储设备不支持主机操作或只为主机操作提供部分支持时，主机将恢复到其本机方法以执行不支持的操作。

关闭硬件加速

如果存储设备不支持硬件加速功能，可以使用 vSphere Client 高级设置将其关闭。

与任何高级设置一样，在禁用硬件加速之前，请咨询 VMware 支持团队。

步骤

1. 在 vSphere Client 的“清单”面板中，选择主机。
2. 单击**配置**选项卡，然后在**软件**下单击**高级设置**。
3. 单击 VMFS3 并将 **VMFS3.HardwareAcceleratedLocking** 字段中的值更改为零。
4. 单击 **DataMover** 并将以下每个字段中的值更改为零：
   - **DataMover.HardwareAcceleratedMove**
   - **DataMover.HardwareAcceleratedInit**
5. 单击**确定**保存更改。

精简置备

创建虚拟机时，会在数据存储上置备一定量的存储空间，或为虚拟磁盘文件分配一定量的存储空间。

默认情况下，当您在创建期间估计虚拟机在其整个生命周期所需的存储空间、为其虚拟磁盘置备固定量的存储空间，并将整个置备空间提交到虚拟磁盘时，ESX 会提供传统的存储置备方法。立即占据整个置备空间的虚拟磁盘叫做厚磁盘。以厚格式创建虚拟磁盘会导致无法充分利用数据存储容量，因为预分配给各个虚拟机的大量存储空间可能仍然未被使用。

为了帮助您避免超额分配存储空间并节省空间，ESX 支持精简置备，它允许您在开始时使用当前所需大小的存储空间，并在以后添加所需的存储空间量。使用 ESX 精简置备功能，可以采用精简格式创建虚拟磁盘。对于精简虚拟磁盘，ESX 会为磁盘当前和未来的活动置备所需的整个空间，但是开始时仅提供磁盘初始操作所需的存储空间大小。

关于虚拟磁盘格式

当执行某些虚拟机管理操作（如创建虚拟磁盘，将虚拟机克隆到模板，或迁移虚拟机）时，可以指定虚拟磁盘文件的格式。

支持以下磁盘格式。如果磁盘驻留在 NFS 数据存储上，则不能指定磁盘格式。NFS 服务器会确定磁盘的分配策略。

精简置备格式

使用此格式可节省存储空间。对于精简磁盘，可以根据所输入的磁盘大小值置备磁盘所需的任意数据存储空间。但是，精简磁盘开始时很小，只使用与初始操作实际所需的大小完全相同的存储空间。

注意 如果虚拟磁盘支持群集解决方案（如容错），则不能将磁盘设置为精简格式。

如果精简磁盘以后需要更多空间，它可以增长到其最大容量，并占据为其置备的整个数据存储空间。而且，您可以将精简磁盘手动转换为厚磁盘。

厚格式

这是默认的虚拟磁盘格式。厚虚拟磁盘不更改大小，并且一开始就占据为其配置的整个数据存储空间。不能将厚磁盘转换为精简磁盘。

创建精简置备虚拟磁盘

当需要节省存储空间时，可以创建精简置备格式的虚拟磁盘。精简置备虚拟磁盘开始时很小，它会在需要更多磁盘空间时增长。

此过程假定您正在使用新建虚拟机向导创建典型或自定义虚拟机。

前提条件

只能在支持精简置备的数据存储上创建精简磁盘。如果磁盘驻留在 NFS 数据存储上，则无法指定磁盘格式，因为 NFS 服务器确定了磁盘的分配策略。

步骤

◆ 在“创建磁盘”对话框中，选择**按需分配和提交空间(精简置备)**。

将创建精简格式的虚拟磁盘。如果未选择“精简置备”选项，则虚拟磁盘将使用默认的厚格式。

下一步

如果创建了精简格式的虚拟磁盘，则以后可以将其增加到最大大小。

查看虚拟机存储资源

可以查看虚拟机的数据存储存储空间的分配方式。

步骤

1 在清单中选择虚拟机。
2 单击**摘要**选项卡。
3 在“资源”部分中检查空间分配信息。
   - 置备的存储 – 保证分配给虚拟机的数据存储空间。如果虚拟机具有精简置备格式的磁盘，则虚拟机可能未使用全部磁盘空间。其他虚拟机可以占用任何未使用的空间。
   - 未共享的存储 – 显示由虚拟机占用且不与其他任何虚拟机共享的数据存储空间。
   - 已使用的存储 – 显示虚拟机文件（包括配置文件、日志文件、快照、虚拟磁盘等等）实际占用的数据存储空间。当虚拟机正在运行时，使用的存储空间还包括交换文件。

确定虚拟机的磁盘格式

可以确定虚拟磁盘是厚格式还是精简格式。

步骤

1 在清单中选择虚拟机。

2 单击**编辑设置**以显示“虚拟机属性”对话框。

3 单击**硬件**选项卡，然后在“硬件”列表中选择相应的硬盘。

   右侧的“磁盘置备”区域将显示虚拟磁盘的类型，可能是“精简”或“厚”。

4 单击**确定**。

下一步

如果虚拟磁盘为精简格式，则可以将其扩充到其最大容量。

将虚拟磁盘从精简磁盘转换为厚磁盘

如果创建的是精简格式的虚拟磁盘，可以将该磁盘转换为厚磁盘。

步骤

1 在清单中选择虚拟机。

2 单击**摘要**选项卡，然后在“资源”下，双击虚拟机的数据存储以打开“数据存储浏览器”对话框。

3 单击虚拟机文件夹以找到要转换的虚拟磁盘文件。虚拟磁盘文件的扩展名为 `.vmdk`。

4 右键单击虚拟磁盘文件，然后选择**扩充**。

厚格式的虚拟磁盘将占据最初为其置备的整个数据存储空间。

处理数据存储超额订购

由于为精简磁盘置备的空间可能大于提交的空间，因此可能发生数据存储超额订购，从而导致数据存储上的虚拟机磁盘总置备空间超过实际容量。

通常，所有附带精简磁盘的虚拟机不会同时需要整个置备数据存储空间，因此可能发生超额订购。但是，如果要避免数据存储超额订购，则可以设置警报，它会在置备空间达到特定阈值时通知您。

有关设置警报的信息，请参见《vSphere 数据中心管理指南》。

如果虚拟机需要更多空间，则根据先来先服务的原则分配数据存储空间。当数据存储空间不足时，可以添加更多的物理存储器，并增加数据存储空间。

请参见第 105 页，“增加 VMFS 数据存储”。

关闭 vCenter Server 存储筛选器

在执行 VMFS 数据存储管理操作时，vCenter Server 使用默认存储筛选器。这些筛选器可以仅检索可用于特定操作的存储设备或 LUN，从而能更有效地避免存储设备损坏。不适合的 LUN 不会显示出来供选择。可以关闭筛选器来查看所有 LUN。

在对 LUN 筛选器进行任何更改之前，请咨询 VMware 支持团队。仅当您有其他方法来防止 LUN 损坏时，才可关闭筛选器。

步骤

1 在 vSphere Client 中，选择**管理 > vCenter Server 设置**。

2 在设置列表中，选择**高级设置**。

3 在**键**文本框中，键入键。

键	筛选器名称
config.vpxd.filter.vmfsFilter	VMFS 筛选器
config.vpxd.filter.rdmFilter	RDM 筛选器
config.vpxd.filter.SameHostAndTransportsFilter	相同主机和传输筛选器
config.vpxd.filter.hostRescanFilter	主机重新扫描筛选器 **注意** 如果关闭“主机重新扫描筛选器”，则每次将一个新的 LUN 提供给主机或群集时，主机仍继续执行重新扫描。

4 在**值**文本框中，为指定的键键入 `False`。

5 单击**添加**。

6 单击**确定**。

无需重新启动 vCenter Server 系统。

vCenter Server 存储筛选

vCenter Server 提供存储筛选器，来帮助您避免由于使用不支持的 LUN 可能导致的存储设备损坏或性能下降。默认情况下，这些筛选器可用。

表 9–2 存储筛选器

筛选器名称	描述	键
VMFS 筛选器	筛选出在 vCenter Server 管理的任何主机上已由 VMFS 数据存储使用的存储设备或 LUN。LUN 不会以要格式化为另一个 VMFS 数据存储或要用作 RDM 的候选者的身份显示。	config.vpxd.filter.vmfsFilter
RDM 筛选器	筛选出在 vCenter Server 管理的任何主机上已由 RDM 引用的 LUN。LUN 不会以要格式化为 VMFS 或要供其他 RDM 使用的候选者的身份显示。 如果需要虚拟机访问相同的 LUN，则虚拟机必须共享相同的 RDM 映射文件。有关此类配置的信息，请参阅《故障切换群集和 Microsoft 群集服务的设置》。	config.vpxd.filter.rdmFilter
相同主机和传输筛选器	筛选出由于主机或存储类型不兼容而不适合用作 VMFS 数据存储区的 LUN。防止将以下 LUN 添加为数据区： ■ 未对共享原始 VMFS 数据存储的所有主机公开的 LUN。 ■ 使用不同于原始 VMFS 数据存储使用的存储类型的 LUN。例如，无法将光纤通道数据区添加到本地存储设备上的 VMFS 数据存储。	config.vpxd.filter.SameHostAndTransportsFilter
主机重新扫描筛选器	在执行数据存储管理操作之后，自动重新扫描和更新 VMFS 数据存储。该筛选器可帮助提供 vCenter Server 管理的所有主机上的所有 VMFS 数据存储的一致视图。 **注意** 如果将一个新的 LUN 提供给主机或群集，则无论是否打开了“主机重新扫描筛选器”，主机都会自动执行重新扫描。	config.vpxd.filter.hostRescanFilter

裸设备映射 10

裸设备映射 (RDM) 为虚拟机提供了一种机制，来直接访问物理存储子系统（仅限光纤通道或 iSCSI）上的 LUN。

以下主题包含 RDM 的相关信息，并且说明如何创建和管理 RDM。

本章讨论了以下主题：

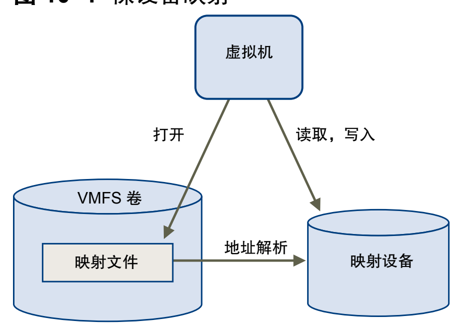
关于裸设备映射

RDM 是独立 VMFS 卷中的映射文件，它可充当裸物理存储设备的代理。RDM 允许虚拟机直接访问和使用存储设备。RDM 包含用于管理和重定向对物理设备进行磁盘访问的元数据。

该文件具有直接访问物理设备的一些优点，同时保留了 VMFS 中虚拟磁盘的一些优点。因此，它可以将 VMFS 易管理性结合到裸机访问中。

RDM 可以用“将裸设备映射到数据存储”、“映射系统 LUN”或“将磁盘文件映射到物理磁盘卷”等短语来描述。所有这些短语均指 RDM。

图 10–1 裸设备映射



尽管 VMware 建议针对大多数虚拟磁盘存储器使用 VMFS 数据存储，但在特定情况下，您可能需要使用原始 LUN，或者使用位于 SAN 中的逻辑磁盘。

例如，在以下情况下，需要使用原始 LUN 处理 RDM：

- 当在虚拟机中运行 SAN 快照或其他分层应用程序时。RDM 通过使用 SAN 特有功能可以更好地启用可扩展备份卸载系统。
- 在任何跨物理主机的 MSCS 群集情况下 — 虚拟到虚拟群集以及物理到虚拟群集。在此情况下，群集数据和仲裁磁盘应配置为 RDM 而非共享 VMFS 上的文件。

将 RDM 视为从 VMFS 卷到原始 LUN 的符号链接。映射使 LUN 显示为 VMFS 卷中的文件。在虚拟机配置中引用 RDM 而非原始 LUN。RDM 包含对原始 LUN 的引用。

使用 RDM，可以：

- 使用 vMotion 迁移具有原始 LUN 的虚拟机。
- 使用 vSphere Client 将原始 LUN 添加到虚拟机。
- 使用分布式文件锁定、权限和命名等文件系统功能。

RDM 有两种可用兼容模式：

- 虚拟兼容模式允许 RDM 的功能与虚拟磁盘文件完全相同，包括使用快照。
- 对于需要较低级别控制的应用程序，物理兼容模式允许直接访问 SCSI 设备。

裸设备映射的优点

RDM 具有许多优点，但并非在每种情况下都适用。通常，对于易管理性而言，虚拟磁盘文件优于 RDM。但是，当需要裸设备时，必须使用 RDM。

RDM 提供几个好处。

用户友好的持久名称

为所映射的设备提供用户友好的名称。使用 RDM 时，不必通过设备名称引用设备。可以根据映射文件的名称来引用设备，例如：

```
/vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
```

动态名称解析

为各个映射设备存储唯一的标识信息。VMFS 将每个 RDM 与其当前的 SCSI 设备相关联，而不考虑由于适配器硬件更改、路径更改、设备重定位等所引起的服务器物理配置的变化。

分布式文件锁定

使为 SCSI 裸设备使用 VMFS 分布式锁定成为可能。当位于不同服务器上的两个虚拟机试图访问同一 LUN 时，RDM 上的分布式锁定使其能够安全使用共享裸 LUN 而不会丢失数据。

文件权限

使文件权限成为可能。在文件打开时，强制执行映射文件权限，以保护映射的卷。

文件系统操作

通过将映射文件作为代理，可以实现使用文件系统实用程序处理映射的卷。对普通文件有效的大部分操作都可应用于映射文件，并且可重定向在映射设备上进行操作。

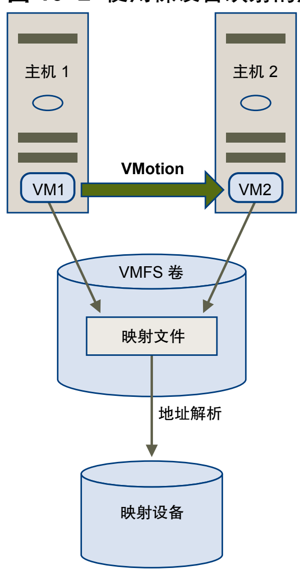
快照

使在映射的卷上使用虚拟机快照成为可能。在物理兼容模式下使用 RDM 时，快照不可用。

vMotion

允许通过 vMotion 迁移虚拟机。映射文件可充当代理，允许 vCenter Server 使用与迁移虚拟磁盘文件相同的机制迁移虚拟机。

图 10–2 使用裸设备映射的虚拟机的 vMotion



SAN 管理代理

使在虚拟机内运行某些 SAN 管理代理成为可能。与此相似，可以在虚拟机内运行需要使用硬件特定 SCSI 命令访问设备的任何软件。这种软件称为基于 SCSI 目标的软件。使用 SAN 管理代理时，需要为 RDM 选择物理兼容模式。

N-Port ID 虚拟化 (NPIV)

令使用 NPIV 技术成为可能，通过该技术，单一光纤通道 HBA 端口可使用多个全球端口名称 (WWPN) 向光纤通道架构注册。通过此功能，HBA 端口可显示为多个虚拟端口，每个端口均有其自身的 ID 和虚拟端口名称。因此，虚拟机就可声明其中每个虚拟端口，并将其用于所有 RDM 流量。

注意 只能将 NPIV 用于具备 RDM 磁盘的虚拟机。

VMware 与存储器管理软件的供应商合作，确保他们的软件能够在包括 ESX 的环境下正常工作。下面是一些这种类型的应用程序：

- SAN 管理软件
- 存储资源管理 (SRM) 软件
- 快照软件
- 复制软件

此类软件将物理兼容模式用于 RDM，以便能够直接访问 SCSI 设备。

各种管理产品都可以完美地集中运行（而不是在 ESX 计算机上运行），而其他产品则可以在服务控制台或虚拟机中良好运行。VMware 未正式认可这些应用程序，也未提供兼容性列表。要了解在 ESX 环境中是否支持某个 SAN 管理应用程序，请与该 SAN 管理软件的提供商联系。

裸设备映射的限制

在使用 RDM 时存在一定的限制。

- 不适用于块设备或某些 RAID 设备 - RDM 使用 SCSI 序列号标识映射设备。由于块设备和某些直连 RAID 设备不能导出序列号，因此不能将其用于 RDM。
- 仅适用于 VMFS-2 和 VMFS-3 卷 – RDM 需要 VMFS-2 或 VMFS-3 格式。在 ESX 中，VMFS-2 文件系统为只读。要使用 VMFS-2 所存储的文件，请将其升级到 VMFS-3。

- 物理兼容模式下无快照 – 如果在物理兼容模式下使用 RDM，则不能使用磁盘快照。物理兼容模式允许虚拟机管理自己的快照或镜像操作。

  在虚拟模式下，可以使用快照。

- 无分区映射 – RDM 要求映射设备是完整的 LUN。不支持映射到分区。

裸设备映射特性

RDM 是 VMFS 卷中管理映射设备元数据的一种特殊映射文件。管理软件将映射文件视作普通磁盘文件，可用于常规文件系统操作。对于虚拟机，存储器虚拟化层将映射设备显示为虚拟 SCSI 设备。

映射文件中元数据的主要内容包括映射设备的位置（名称解析）、映射设备的锁定状况和权限，等等。

RDM 虚拟兼容模式和物理兼容模式

可以在虚拟兼容或物理兼容模式中使用 RDM。虚拟模式指定映射设备的完整虚拟化。物理模式指定映射设备的最小 SCSI 虚拟化，实现了 SAN 管理软件的最大灵活性。

在虚拟模式下，VMkernel 只将 READ 和 WRITE 发送到映射设备。映射的设备在客户机操作系统中的出现形式与虚拟磁盘文件在 VMFS 卷中的形式完全相同。隐藏真正的硬件特性。如果您正在虚拟模式中使用裸磁盘，您能够认识到 VMFS 的优点，例如，用于保护数据的高级文件锁定和用于简化开发流程的快照等。虚拟模式比物理模式在存储硬件上的移植性更强，表现出来的行为与虚拟磁盘文件相同。

在物理模式下，Vmkernel 将所有 SCSI 命令传递至设备。例外：REPORT LUN 命令被虚拟化，以便 VMkernel 可将 LUN 隔离到所属的虚拟机中。否则，基础硬件的所有物理特性都将显示出来。物理模式对于在虚拟机中运行 SAN 管理代理或其他基于 SCSI 目标的软件非常有用。物理模式还允许虚拟到物理群集，实现具有成本效益的高可用性。

动态名称解析

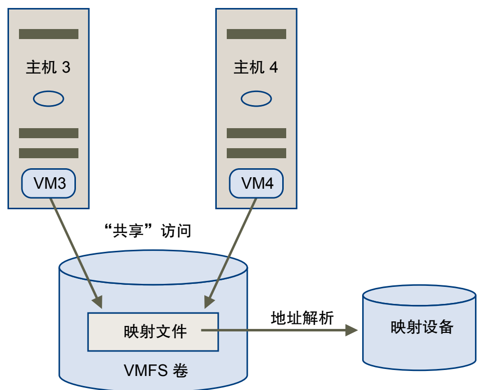
RDM 文件支持动态名称解析（裸设备的路径发生更改时）。

所有映射的存储设备都由 VMFS 进行唯一标识，并且标识存储在其内部数据结构中。裸设备路径中的任何更改（如光纤通道交换机发生故障或添加新的 HBA）都可以造成设备名称发生变化。动态名称解析可解析这些更改，并将原始设备与其新名称自动关联起来。

虚拟机群集的裸设备映射

对需要访问同一原始 LUN 以实施故障切换方案的虚拟机群集执行 RDM。其设置与访问同一虚拟磁盘文件的虚拟机群集的设置相同，但 RDM 会替换虚拟磁盘文件。

图 10–3 从群集虚拟机进行访问



比较可用的 SCSI 设备访问模式

访问基于 SCSI 的存储设备的方法包括 VMFS 数据存储上的虚拟磁盘文件、虚拟模式 RDM 和物理模式 RDM。

为了帮助您在 SCSI 设备的可用访问模式之间进行选择，表 10‑1 提供了对不同模式可用功能的快速比较。

表 10‑1 虚拟磁盘和裸设备映射的可用功能

ESX 功能	虚拟磁盘文件	虚拟模式 RDM	物理模式 RDM
SCSI 命令已传递	否	否	是 不传递 REPORT LUN
vCenter Server 支持	是	是	是
快照	是	是	否
分布式锁定	是	是	是
群集	仅限机箱内群集	机箱内群集和机箱间群集	物理到虚拟群集
基于 SCSI 目标的软件	否	否	是

VMware 建议将虚拟磁盘文件用于群集中的机箱内群集类型。如果计划将机箱内群集重新配置为机箱间群集，请为机箱内群集采用虚拟模式 RDM。

管理映射的 LUN

使用 vSphere Client，可以将 SAN LUN 映射到数据存储，并管理指向映射 LUN 的路径。

其他可用于管理映射 LUN 及其 RDM 的工具包括 `vmkfstools` 实用程序以及由 vSphere CLI 使用的其他命令。可以使用 `vmkfstools` 实用程序来执行 vSphere Client 可用的许多相同操作。

还可以在服务控制台中使用常用文件系统命令。

使用 RDM 创建虚拟机

授予虚拟机对原始 SAN LUN 的直接访问权限时，创建驻留在 VMFS 数据存储上并指向 LUN 的映射文件 (RDM)。尽管映射文件与常规虚拟磁盘文件的扩展名均为 `.vmdk`，但 RDM 文件仅包括映射信息。实际虚拟磁盘数据直接存储在 LUN 上。

您可创建 RDM 作为新虚拟机的初始磁盘，或将其添加到现有虚拟机中。创建 RDM 时，可以指定要映射的 LUN 以及要用来放置 RDM 的数据存储。

步骤

1 遵循在创建自定义虚拟机时所需的全部步骤。

2 在“选择磁盘”页面中，选择**裸设备映射**，然后单击**下一步**。

3 在 SAN 磁盘或 LUN 列表中，选择您的虚拟机可直接访问的原始 LUN。

4 为 RDM 映射文件选择数据存储。

   可以将 RDM 文件置于虚拟机配置文件所驻留的同一数据存储上，也可以选择不同的数据存储。

   注意 要将 vMotion 用于启用了 NPIV 的虚拟机，请确保该虚拟机的 RDM 文件位于同一数据存储上。启用 NPIV 后，无法在数据存储之间执行 Storage vMotion 或 vMotion。

5 选择兼容模式。

选项	描述
物理	允许客户机操作系统直接访问硬件。如果正在虚拟机中使用 SAN 感知应用程序，则物理兼容模式非常有用。但是，如果迁移过程涉及到复制磁盘，则使用进行了物理兼容性配置的 RDM 的已启动虚拟机无法迁移。此类虚拟机无法克隆，也无法克隆为模板。
虚拟	允许 RDM 像虚拟磁盘一样工作，因此您可以使用快照和克隆之类的功能。

6 选择虚拟设备节点。

7 如果选择独立模式，则选择下列一项：

选项	描述
持久	更改会立即永久性地写入磁盘。
非持久	关闭电源或恢复快照时，会放弃对该磁盘的更改。

8 单击**下一步**。

9 在“即将完成新建虚拟机”页面上，检查您所做的选择。

10 单击**完成**完成虚拟机。

管理映射的原始 LUN 的路径

可以管理映射的原始 LUN 的路径。

步骤

1 以管理员或映射磁盘所属的虚拟机的所有者身份登录。

2 在“清单”面板中选择虚拟机。

3 在**摘要**选项卡中，单击**编辑设置**。

4 在**硬件**选项卡上，选择**硬盘**，然后单击**管理路径**。

5 使用“管理路径”对话框启用或禁用路径、设置多路径策略并指定首选的路径。

有关管理路径的信息，请参见第 109 页，“在 ESX 中使用多路径”。

安全

ESX 系统的安全 11

ESX 的开发注重于加强安全性。VMware 从安全角度出发，确保 ESX 环境和地址系统架构中的安全。

本章讨论了以下主题：

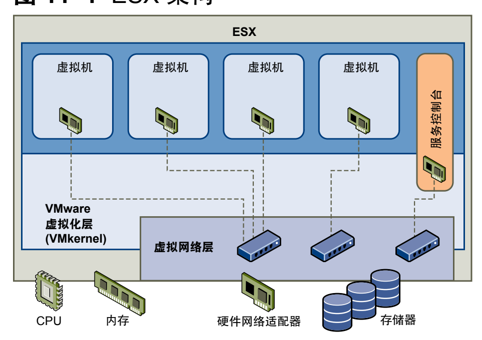
ESX 架构和安全功能

ESX 的组件和整体架构专用于确保 ESX 系统的整体安全性。

从安全角度而言，ESX 主要由四个组件组成：虚拟化层、虚拟机、服务控制台和虚拟网络连接层。

图 11–1 提供这些组件的概述。

图 11–1 ESX 架构



安全和虚拟化层

VMware 设计了虚拟化层（或 VMkernel）来运行虚拟机。它控制着主机所使用的硬件，并调度虚拟机之间的硬件资源分配。由于 VMkernel 专用于支持虚拟机而不用于其他用途，因此其接口严格限制在管理虚拟机所需的 API。

ESX 提供具有以下功能的附加 VMkernel 保护：

内存强化安全　　将 ESX 内核、用户模式应用程序及可执行组件（如驱动程序和库）位于无法预测的随机内存地址中。在将该功能与微处理器提供的不可执行的内存保护结合使用时，可以提供保护，使恶意代码很难通过内存漏洞来利用系统漏洞。

内核模块完整性　　数字签名确保由 VMkernel 加载的模块、驱动程序及应用程序的完整性和真实性。模块签名允许 ESX 识别模块、驱动程序或应用程序的提供商以及它们是否通过 VMware 认证。

安全和虚拟机

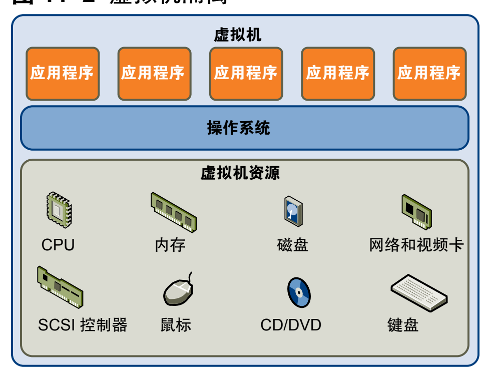
虚拟机是运行应用程序和客户机操作系统的容器。在设计上，所有的 VMware 虚拟机均互相隔离。通过此隔离，多个虚拟机就可在共享硬件的同时安全地运行，既确保能够访问硬件，又保证运行不受干扰。

如果没有 ESX 系统管理员明确授予的特权，即使是在虚拟机的客户机操作系统上具有系统管理员特权的用户，也无法突破该隔离层来访问另一台虚拟机。如果某个虚拟机上的客户机操作系统运行时发生故障，则虚拟机隔离将确保同一台主机上的其他虚拟机可以继续运行。客户机操作系统故障不影响：

- 用户访问其他虚拟机的能力
- 正常运行的虚拟机访问其所需资源的能力
- 其他虚拟机的性能

同一硬件上运行的虚拟机互相隔离。虽然虚拟机共享诸如 CPU、内存及 I/O 设备之类的物理资源，但单一虚拟机上的客户机操作系统可检测到的设备仅限于可供其使用的虚拟设备，如图 11–2 中所示。

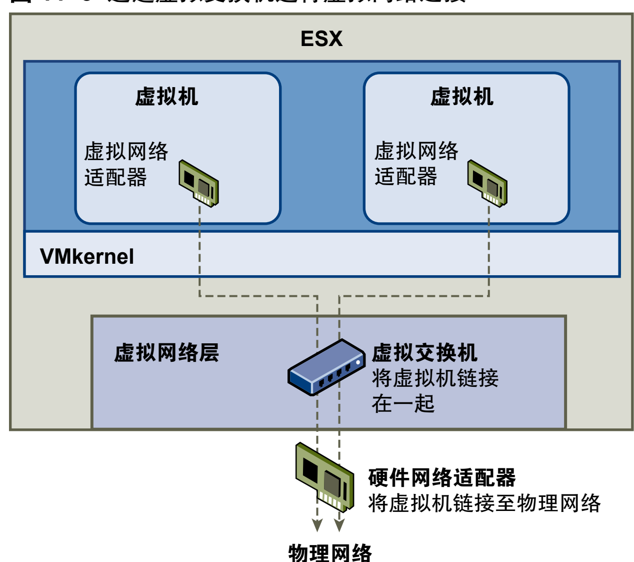
图 11–2 虚拟机隔离



由于 VMkernel 可调节物理资源及通过其对物理硬件进行的所有访问，因此虚拟机无法阻止此层隔离。

如同物理机通过网卡就可与网络中其他计算机进行通信一样，虚拟机也可以通过虚拟交换机与同一台主机上运行的其他虚拟机进行通信。而且，虚拟机可通过物理网络适配器与物理网络（包括其他 ESX 主机上的虚拟机）进行通信，如图 11–3 中所示。

图 11–3 通过虚拟交换机进行虚拟网络连接



这些特性适用于网络环境中的虚拟机隔离：

- 如果某个虚拟机未与任何其他虚拟机共享虚拟交换机，则该虚拟机与主机中的虚拟网络完全隔离。
- 如果没有为某个虚拟机配置物理网络适配器，则该虚拟机与任何物理网络完全隔离。
- 如果使用了与保护物理机相同的保护措施（防火墙和防毒软件等）来保护网络中的虚拟机，该虚拟机则与物理机一样安全。

在主机上设置资源预留和限制，可进一步保护虚拟机。例如，通过 ESX 中可用的详细资源控制配置虚拟机，以便其获得的主机 CPU 资源始终不少于 10%，但也决不超过 20%。

资源预留和限制可防止虚拟机的性能因其他虚拟机消耗过多的共享硬件资源而降低。例如，如果主机上的一台虚拟机由于受到拒绝服务 (DoS) 攻击而出现故障，该虚拟机上的资源限制就会阻止该攻击占据太多硬件资源，否则其他虚拟机也会受到影响。与此相似，每台虚拟机上的资源预留可在受到 DoS 攻击的虚拟机需要较多资源的情况下确保所有其他虚拟机仍有足够的资源可供使用。

默认情况下，ESX 通过应用分布式算法而强制实行一种形式的资源预留，该分布算法将可用主机资源均匀分布于虚拟机之间，同时保留一定百分比的资源供其他系统组件（如服务控制台）使用。此默认行为在一定程度上为防止 DoS 和分布式拒绝服务 (DDoS) 攻击提供了自然保护。要自定义默认行为，以避免在虚拟机配置之间均匀分布资源预留和限制，可逐一指定资源预留和限制。

安全和虚拟网络连接层

虚拟网络连接层包括虚拟网络适配器和虚拟交换机。ESX 依赖于虚拟网络连接层来支持虚拟机及其用户之间的通信。此外，主机可使用虚拟网络连接层与 iSCSI SAN 和 NAS 存储器等进行通信。

可确保虚拟机网络安全的方法取决于所安装的客户机操作系统、虚拟机是否运行于可信环境及各种其他因素。与其他常见安全措施（例如，安装防火墙）结合使用时，虚拟交换机的保护作用会大大加强。

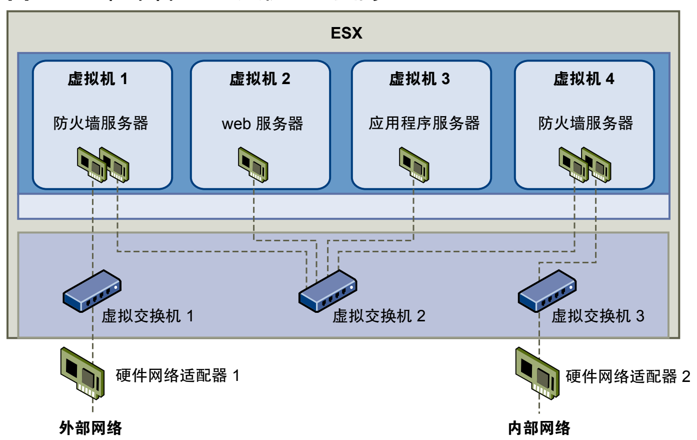
ESX 还支持可用于为虚拟机网络、服务控制台或存储器配置提供进一步保护的 IEEE 802.1q VLAN。通过 VLAN，可对物理网络进行分段，以便使同一物理网络中的两台计算机无法互相收发数据包，除非它们位于同一 VLAN 上。

在单台 ESX 主机上创建网络 DMZ

在单台主机上创建网络隔离区 (DMZ) 是使用 ESX 隔离和虚拟网络功能配置安全环境的一个示例。

图 11-4 显示了配置。

图 11–4 在单台 ESX 主机上配置的 DMZ



在此示例中，将四台虚拟机配置为在虚拟交换机 2 上创建虚拟 DMZ：

- 虚拟机 1 和虚拟机 4 运行防火墙，并通过虚拟交换机连接虚拟适配器。这两个虚拟机都是多址的。
- 虚拟机 2 运行 Web 服务器，同时虚拟机 3 作为应用程序服务器运行。这两个虚拟机都是单址的。

Web 服务器和应用程序服务器占用两个防火墙之间的 DMZ。这两个元素之间的媒介是用来连接防火墙和服务器的虚拟交换机 2。此交换机未与 DMZ 之外的任何元素进行直接连接，且通过两个防火墙与外部流量相隔离。

从运行角度来看，外部流量通过硬件网络适配器 1（由虚拟交换机 1 路由）从 Internet 进入虚拟机 1，并由此虚拟机上安装的防火墙进行验证。如果经防火墙授权，流量可路由至 DMZ 中的虚拟交换机，即虚拟交换机 2。由于 Web 服务器和应用程序服务器也连接至此交换机，因此，它们可以满足外部请求。

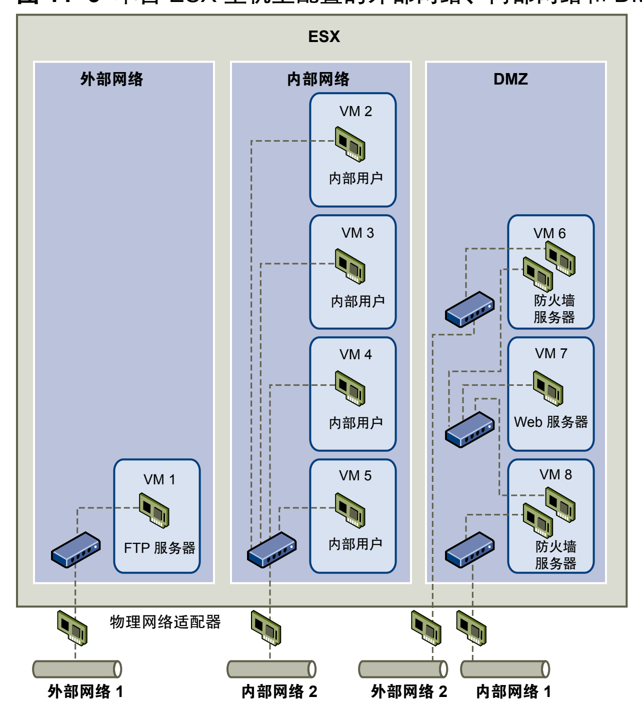
虚拟交换机 2 还与虚拟机 4 相连。此虚拟机在 DMZ 和内部企业网络之间提供防火墙。此防火墙对来自 Web 服务器和应用程序服务器的数据包进行筛选。验证后的数据包将通过虚拟交换机 3 路由至硬件网络适配器 2。硬件网络适配器 2 与内部企业网络相连。

在单台主机上创建 DMZ 时，可使用相当轻量的防火墙。尽管此配置中的虚拟机无法直接控制其他虚拟机或访问其内存，但是所有虚拟机仍然通过虚拟网络处于连接状态。此网络可能会传播病毒，或成为其他类型攻击的对象。DMZ 中虚拟机的安全性等同于连接到同一网络的独立物理机。

在单台 ESX 主机中创建多个网络

ESX 系统的设计可让您将一些虚拟机组连接至内部网络，将一些虚拟机组连接至外部网络，再将另一些虚拟机组同时连接至外部网络和内部网络 — 这一切都在同一主机上进行。此功能是由对虚拟机的基本隔离和对虚拟网络连接功能的有计划使用组合而成的。

图 11–5 单台 ESX 主机上配置的外部网络、内部网络和 DMZ



在图 11–5 中，系统管理员将主机配置到三个不同的虚拟机区域中：FTP 服务器、内部虚拟机和 DMZ。每个区域均提供唯一功能。

FTP 服务器

虚拟机 1 是使用 FTP 软件配置的，可作为从外部资源（例如，由供应商本地化的表单和辅助材料）发出及向其发送的数据的存储区域。

此虚拟机仅与外部网络相关联。它自身拥有可用来与外部网络 1 相连接的虚拟交换机和物理网络适配器。此网络专用于公司在从外部来源接收数据时所使用的服务器。例如，公司使用外部网络 1 从供应商接收 FTP 流量，并允许供应商通过 FTP 访问存储在外部可用服务器上的数据。除了服务于虚拟机 1，外部网络 1 也服务于在整个站点内不同 ESX 主机上配置的 FTP 服务器。

由于虚拟机 1 不与主机中的任何虚拟机共享虚拟交换机或物理网络适配器，因此，其他驻留的虚拟机无法通过虚拟机 1 网络收发数据包。此限制可防止嗅探攻击（嗅探攻击需向受害者发送网络流量）。更为重要的是，攻击者再也无法使用 FTP 固有的漏洞来访问任何主机的其他虚拟机。

内部虚拟机

虚拟机 2 至 5 仅供内部使用。这些虚拟机用来处理和存储公司机密数据（例如，医疗记录、法律裁决和欺诈调查）。因此，系统管理员必须确保为这些虚拟机提供最高级别的保护。

这些虚拟机通过其自身的虚拟交换机和网络适配器连接到内部网络 2。内部网络 2 仅供内部人员使用（例如，索赔专员、内部律师或调解员）。

虚拟机 2 至 5 可通过虚拟交换机与另一个虚拟机进行通信，也可通过物理网络适配器与内部网络 2 上其他位置的内部虚拟机进行通信。它们不能与对外计算机进行通信。如同 FTP 服务器一样，这些虚拟机不能通过其他虚拟机网络收发数据包。同样，主机的其他虚拟机不能通过虚拟机 2 至 5 收发数据包。

DMZ

虚拟机 6 至 8 配置为可供营销小组用于发布公司外部网站的 DMZ。

这组虚拟机与外部网络 2 和内部网络 1 相关联。公司使用外部网络 2 来支持营销部门和财务部门用来托管公司网站的 Web 服务器及公司为外部用户托管的其他 Web 设施。内部网络 1 是营销部门用于向公司网站发布内容、张贴下载内容及维护服务（例如，用户论坛）的媒介。

由于这些网络与外部网络 1 和内部网络 2 相隔离，因此虚拟机无任何共享联络点（交换机或适配器），FTP 服务器或内部虚拟机组也不存在任何攻击风险。

通过利用虚拟机隔离、正确配置虚拟交换机及维护网络独立，系统管理员可在同一 ESX 主机上容纳全部三个虚拟机区域，而且不用担心数据或资源受到破坏。

公司使用多个内部和外部网络，并确保每组的虚拟交换机和物理网络适配器与其他组的虚拟交换机和物理网络适配器完全独立，从而在虚拟机组中强制实施隔离。

由于没有任何虚拟交换机横跨虚拟机区域，因此系统管理员可成功地消除虚拟机区域之间的数据包泄漏风险。虚拟机本身无法向另一个虚拟交换机直接泄漏数据包。仅在以下情况下，数据包才会在虚拟交换机之间移动：

- 这些虚拟交换机连接到同一物理 LAN。
- 这些虚拟交换机连接到可用于传输数据包的公用虚拟机。

这些条件均未出现在样本配置中。如果系统管理员要确认不存在公用虚拟交换机路径，可通过在 vSphere Client 或 vSphere Web Access 中查看网络交换机布局，以检查是否可能存在共享联系点。

为了保护虚拟机的资源，系统管理员为每台虚拟机配置了资源预留和限制，从而降低了 DoS 和 DDoS 攻击的风险。系统管理员在 DMZ 的前后端安装了软件防火墙，确保主机受到物理防火墙的保护，并配置了服务控制台和联网的存储器资源以使每个资源均有其自己的虚拟交换机，从而为 ESX 主机和虚拟机提供进一步保护。

安全和服务控制台

ESX 服务控制台是基于 Red Hat Enterprise Linux 5 (RHEL5) 的 Linux 有限版本。服务控制台为监控和管理整个 ESX 主机提供了执行环境。

如果服务控制台因某种原因受到威胁，与其进行交互的虚拟机也可能受到威胁。为了使通过服务控制台进行攻击的风险最小化，VMware 使用防火墙对服务控制台进行保护。

除了实施服务控制台防火墙外，VMware 还使用其他方法降低服务控制台的风险。

- ESX 仅运行管理其功能所不可或缺的服务，而且分发仅限于运行 ESX 所需的功能。
- 默认情况下，ESX 安装时的设置为高安全性设置。所有出站端口都已关闭，只有打开的入站端口是与客户端（如 vSphere Client）进行交互所需的端口。保留此安全设置，除非服务控制台连接到可信网络。

- 默认情况下，并非专用于对服务控制台进行管理访问的所有端口均处于关闭状态。如果需要其他服务，则必须专门打开相应的端口。
- 默认情况下，弱密码被禁用，来自客户端的所有通信都通过 SSL 进行保护。用于保护通道安全的确切算法取决于 SSL 握手。在 ESX 上创建的默认证书使用带有 RSA 加密的 SHA-1 作为签名算法。
- ESX 在内部使用 Tomcat Web 服务来支持 Web 客户端（如 vSphere Web Access）对服务控制台进行的访问。经过修改，Tomcat Web 服务仅运行 Web 客户端进行管理和监控所需的功能。因此，ESX 不易遇到在广泛使用中所发现的 Tomcat 安全问题。
- VMware 监控可能影响服务控制台安全性的所有安全警示，并在必要时提供安全修补程序，就如同为可能影响 ESX 主机的任何其他安全漏洞提供该安全修补程序一样。VMware 为 RHEL 5 和更高版本提供安全修补程序（如果可用的话）。
- 未安装诸如 FTP 和 Telnet 之类的不安全服务，且这些服务的端口在默认情况下是关闭的。由于 SSH 和 SFTP 之类较为安全的服务易于获取，因此，请始终避免使用这些不安全的服务来支持更为安全的替代方案。如果必须使用不安全的服务，且已为服务控制台实施了充分的保护措施，则必须明确打开相应端口才能支持这些服务。
- 使用 `setuid` 或 `setgid` 标记的应用程序数量已最小化。可以禁用 ESX 操作可选的任何 `setuid` 或 `setgid` 应用程序。

尽管可以在服务控制台上安装和运行专用于 RHEL 5 的某些类型的程序，但这一用法不受支持，除非 VMware 另有明确说明。如果在受支持的配置中发现安全漏洞，VMware 会主动通知已签署有效支持和订购合同的所有客户，并提供所有必要的修补程序。

注意 请仅执行 http://www.vmware.com/security/ 中的 VMware 安全建议。不要执行由 Red Hat 发布的安全建议。

安全资源和信息

可以在 VMware 网站上查找其他的安全相关信息。

表 11-1 列出了安全主题以及这些主题的其他信息的所在位置。

表 11-1 Web 上的 VMware 安全资源

主题	资源
VMware 安全策略、最新安全预警、安全下载及安全主题重点讨论	http://www.vmware.com/security/
公司安全响应策略	http://www.vmware.com/support/policies/security_response.html VMware 致力于帮助维护安全的环境。安全问题是需要及时更正的。VMware 安全响应策略中作出了解决其产品中可能存在的漏洞之承诺。
第三方软件支持策略	http://www.vmware.com/support/policies/ VMware 支持各种存储系统和软件代理（如备份代理及系统管理代理等）。可以通过在 http://www.vmware.com/vmtn/resources/ 上搜索 ESX 兼容性指南，找到支持 ESX 的代理、工具及其他软件的列表。 VMware 不可能对此行业中的所有产品和配置进行测试。如果 VMware 未在兼容性指南中列出某种产品或配置，其技术支持人员将尝试帮助解决任何相关问题，但不能保证该产品或配置的可用性。请始终对不受支持的产品或配置进行安全风险评估。
VMware 产品认证	http://www.vmware.com/security/certifications/
关于虚拟化和安全性的一般信息	VMware 虚拟安全技术资源中心 http://www.vmware.com/go/security/

表 11–1 Web 上的 VMware 安全资源 （续）

主题	资源
合规性和安全标准，以及关于虚拟化和合规性的合作伙伴解决方案和深入内容	http://www.vmware.com/go/compliance/
关于保护虚拟机的 VMsafe 技术的信息，包括合作伙伴解决方案的列表	http://www.vmware.com/go/vmsafe/

确保 ESX 配置的安全 12

可以采取一些措施为 ESX 主机、虚拟机和 iSCSI SAN 创造安全的环境。从安全角度考虑网络配置规划，还要考虑为了保护配置中的组件免遭攻击而执行的步骤。

本章讨论了以下主题：

使用防火墙确保网络安全

安全管理员使用防火墙保护网络或网络中的选定组件免遭侵袭。

防火墙可控制对其保护范围内的设备的访问，方法是关闭除管理员显式或隐式指定的授权路径之外的所有通信路径。管理员在防火墙打开的路径或端口允许防火墙内外设备间的流量。

在虚拟机环境中，可以为组件之间的防火墙规划布局。

- 物理计算机（如 vCenter Server 主机和 ESX 主机之间）。
- 一个虚拟机与另一个虚拟机（例如在作为外部 Web 服务器的虚拟机与连接公司内部网络的虚拟机之间）。
- 物理机与虚拟机（例如在物理网络适配器卡和虚拟机之间设立防火墙）。

防火墙在 ESX 配置中的使用方式取决于您打算如何使用网络以及如何为给定的组件提供所需的安全。例如，如果在您创建的虚拟网络中的每个虚拟机专用于运行同一部门的不同基准测试套件，那么从一个虚拟机对另一个虚拟机进行不利访问的风险极小。因此，防火墙存在于虚拟机之间的配置不是必需的。但是，为了防止干扰外部主机的测试运行，可对所用配置进行设置，以便在虚拟网络的入口点设有防火墙来保护整组虚拟机。

针对有 vCenter Server 的配置设立防火墙

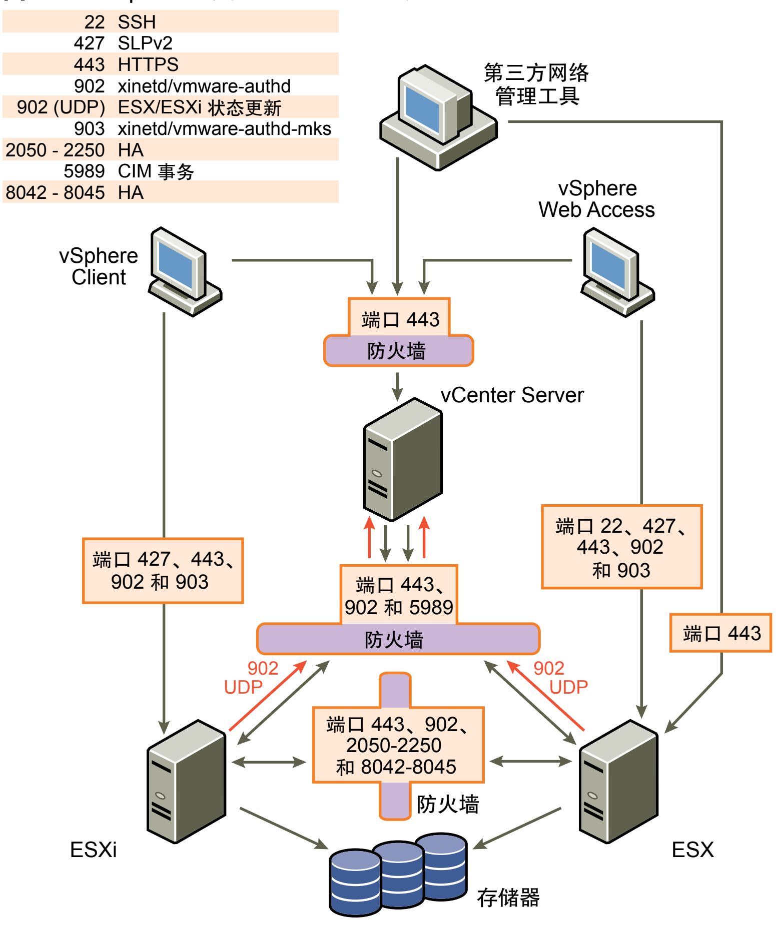
如果通过 vCenter Server 访问 ESX 主机，则通常使用防火墙保护 vCenter Server。该防火墙可为网络提供基本保护。

防火墙可能位于客户端和 vCenter Server 之间。或者，vCenter Server 和客户端可以均受防火墙的保护，这取决于您的部署。重点是确保在您认为的系统入口点有防火墙。

如果使用 vCenter Server，可在图 12-1 中所示的任何位置安装防火墙。根据配置不同，可能无需图中所有防火墙，也可能需要在其他位置安装防火墙。此外，您的配置可能包括可选模块，例如 VMware vCenter Update Manager（此处没有显示）。请参考特定于产品的防火墙设置信息文档，如 Update Manager 文档。

有关 TCP 和 UDP 端口的完整列表，包括用于 VMware vMotion™ 和 VMware 容错的端口，请参见第 143 页，“用于管理访问的 TCP 和 UDP 端口”。

图 12–1 vSphere 网络配置和流量示例



配置了 vCenter Server 的网络可通过几种客户端接收通信：vSphere Client、vSphere Web Access 或使用 SDK 与主机相连接的第三方网络管理客户端。在正常操作期间，vCenter Server 在指定的端口上侦听其受管主机和客户端的数据。vCenter Server 还假设其受管主机在指定的端口上侦听 vCenter Server 的数据。如果任何这些元素之间有防火墙，必须确保防火墙中有打开的端口以支持数据传输。

视您计划如何使用网络及各种设备所需安全级别而定，可能还需要在网络中的许多其他访问点设立防火墙。根据为网络配置确定的安全风险选择防火墙位置。下面列出了 ESX 实施中常用的防火墙位置。列表和图 12–1 中显示的许多防火墙位置都是可选的。

- Web 浏览器与 vSphere Web Access HTTP 和 HTTPS 代理服务器之间。
- vSphere Client、vSphere Web Access Client 或第三方网络管理客户端与 vCenter Server 之间。
- vSphere Client 与 ESX 主机之间（如果用户通过 vSphere Client 访问虚拟机）。此连接是 vSphere Client 与 vCenter Server 之间的附加连接，且需要一个不同的端口。
- Web 浏览器与 ESX 主机之间（如果用户通过 Web 浏览器访问虚拟机）。此连接是 vSphere Web Access Client 与 vCenter Server 之间的附加连接，且需要一个不同的端口。
- vCenter Server 与 ESX 主机之间。

- 网络中的 ESX 主机之间。尽管主机之间的流量通常被认为是可信的，但是，如果您关注计算机的安全漏洞，可在主机间添加防火墙。

  如果在 ESX 主机间添加防火墙并打算在服务器间迁移虚拟机、执行克隆操作或使用 vMotion，还必须在用来将源主机和目标主机隔开的防火墙中打开端口，以便源主机与目标主机进行通信。

- ESX 主机和网络存储器（例如 NFS 或 iSCSI 存储器）之间。这些端口并非专用于 VMware，您可以根据网络规范进行配置。

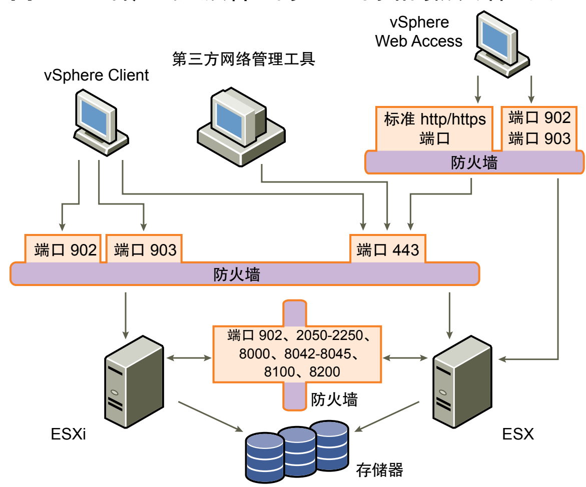
针对没有 vCenter Server 的配置设立防火墙

如果将客户端直接连接到 ESX 网络，而不是使用 vCenter Server，则防火墙的配置略为简单。

可在图 12–2 中显示的任何位置安装防火墙。

注意 根据配置不同，可能无需图中所有防火墙，也可能需在未显示的位置安装防火墙。

图 12–2 客户端直接管理的 ESX 网络的防火墙配置



无论网络有没有配置 vCenter Server，均通过相同类型的客户端接收通信：vSphere Client、第三方网络管理客户端或 vSphere Web Access Client。防火墙需求基本相同，但有一些重要区别。

- 与包含 vCenter Server 的配置一样，应确保有防火墙保护 ESX 层，或保护客户端及 ESX 层，具体取决于您的配置。该防火墙可为网络提供基本保护。所使用的防火墙端口与配置了 vCenter Server 的情况相同。
- 此类配置中的许可证是您在每台主机上安装的 ESX 包的一部分。由于许可功能驻留在服务器上，因此不需要单独的许可证服务器。这就免除了在 License Server 与 ESX 网络间设立防火墙的需要。

通过防火墙连接到 vCenter Server

vCenter Server 使用端口 443 侦听其客户端的数据传输。如果 vCenter Server 及其客户端之间设有防火墙，则必须配置一个可供 vCenter Server 接收其客户端数据的连接。

要使 vCenter Server 接收来自于 vSphere Client 的数据，请在防火墙中打开端口 443，以允许数据从 vSphere Client 传输到 vCenter Server。有关在防火墙中配置端口的其他信息，请联系防火墙系统管理员。

如果正在使用 vSphere Client 且不希望将端口 443 用作 vSphere Client 与 vCenter Server 的通信端口，可通过在 vSphere Client 中更改 vCenter Server 设置来切换到另一个端口。要了解如何更改这些设置，请参见《VMware vSphere 数据中心管理指南》。

通过防火墙连接到虚拟机控制台

无论是通过 vCenter Server 将客户端连接到 ESX 主机，还是将其直接连接到主机，用户和管理员与虚拟机控制台的通信都需要某些端口。这些端口支持不同的客户端功能，与 ESX 上的不同层相连接，并使用不同身份验证协议。

端口 902

vCenter Server 使用此端口将数据发送给 vCenter Server 受管主机。端口 902 是 vCenter Server 向 ESX 主机发送数据时假设可用的端口。

端口 902 通过 VMware 授权守护进程 (`vmware-authd`) 将 vCenter Server 连接至主机。此守护进程将端口 902 的数据分多路传输到适当的接收方进行处理。VMware 不支持为该连接配置其他端口。

端口 443

vSphere Client、vSphere Web Access Client 和 SDK 使用此端口向 vCenter Server 受管主机发送数据。当直接连接到 ESX 主机时，vSphere Client、vSphere Web Access Client 和 SDK 还使用此端口支持与服务器及其虚拟机相关的任何管理功能。端口 443 是客户端向 ESX 主机发送数据时假设可用的端口。VMware 不支持为这些连接配置其他端口。

端口 443 通过 Tomcat Web 服务或 SDK 将客户端连接至 ESX 主机。`vmware-hostd` 将端口 443 的数据分多路传输到适当的接收方进行处理。

端口 903

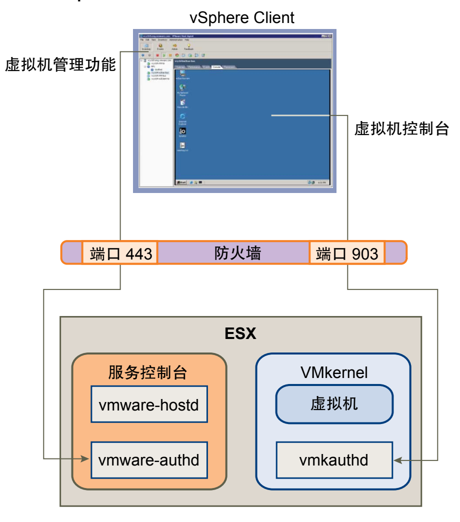
vSphere Client 和 vSphere Web Access 使用此端口为虚拟机上客户机操作系统的 MKS 活动提供连接。用户正是通过此端口与虚拟机的客户机操作系统及应用程序交互。端口 903 是 vSphere Client 和 vSphere Web Access 与虚拟机交互时假设可用的端口。VMware 不支持为此功能配置不同端口。

端口 903 将 vSphere Client 连接到 ESX 上所配置的指定虚拟机。

图 12-3 显示了 vSphere Client 功能、端口及 ESX 进程间的关系。

vSphere Web Access Client 使用相同的基本映射与 ESX 主机交互。

图 12-3 vSphere Client 与 ESX 通信的端口使用情况



如果在 vCenter Server 系统和 vCenter Server 受管主机间设有防火墙，请打开防火墙中的端口 443 和 903 以允许数据从 vCenter Server 传输到 ESX 主机和直接从 vSphere Client 传输到 ESX 主机。

有关配置端口的其他信息，请咨询防火墙系统管理员。

通过防火墙连接到 ESX 主机

如果在两台 ESX 主机间设有防火墙，并希望允许主机间的事务或使用 vCenter Server 执行任何源或目标活动（例如 VMware High Availability (HA) 流量、迁移、克隆或 vMotion），则必须配置一个可供受管主机接收数据的连接。

要配置用于接收数据的连接，请打开以下范围中的端口：

- 443（服务器到服务器的迁移和置备流量）
- 2050 – 2250（用于 HA 流量）
- 8000（用于 vMotion）
- 8042 – 8045（用于 HA 流量）

有关配置端口的其他信息，请咨询防火墙系统管理员。

为支持的服务和管理代理配置防火墙端口

必须在您的环境中配置防火墙，以接受普遍支持的服务。

使用 vSphere Client 配置服务控制台防火墙。在 vCenter Server 中配置 ESX 主机安全配置文件时，添加或移除这些服务或代理会自动打开或关闭防火墙中的预定端口以允许或禁止与这些服务或代理通信。

下面是 vSphere 环境中常见的服务和代理：

- NFS 客户端（不安全服务）
- NTP 客户端
- iSCSI 软件客户端
- CIM HTTP 服务器（不安全服务）
- CIM HTTPS 服务器
- Syslog 客户端
- NFS 服务器（不安全服务）
- NIS 客户端
- SMB 客户端（不安全服务）
- FTP 客户端（不安全服务）
- SSH 客户端
- Telnet 客户端（不安全服务）
- SSH 服务器
- Telnet 服务器（不安全服务）
- FTP 服务器（不安全服务）
- SNMP 服务器
- 您安装的其他受支持的管理代理

注意 此列表可能会更改，因此您可能会发现 vSphere Client 提供的服务和代理在该列表中找不到。此外，并非列表中的所有服务都将默认安装。可能需要执行其他任务来配置和启用这些服务。

如果安装列表中没有的设备、服务或代理，请从命令行打开服务控制台防火墙中的端口。

允许服务或管理代理访问 ESX

可以配置防火墙属性以允许服务或管理代理进行访问。

步骤

1 使用 vSphere Client 登录到 vCenter Server 系统。

2 在“清单”面板中选择主机。

3 依次单击**配置**选项卡和**安全配置文件**。

   vSphere Client 将显示与相应防火墙端口连接的入站和出站活动列表。

4 单击**属性**，打开“防火墙属性”对话框。

   “防火墙属性”对话框列出了可为主机配置的所有服务和管理代理。

5 选择要启用的服务和代理。

   “输入端口”和“输出端口”列表示 vSphere Client 为该服务打开的端口。“协议”列表示该服务使用的协议。“守护进程”列表示与该服务关联的守护进程的状态。

6 单击**确定**。

根据防火墙设置自动执行服务行为

ESX 可对服务是否随防火墙端口状态启动的行为进行自动化。

自动化功能有助于确保当环境配置为启用服务功能时启动服务。例如，仅当某些端口打开时启动某网络服务可帮助避免这样的情况，即服务已启动，但无法完成实现预定目的所需的通信。

另外，某些协议（如 Kerberos）要求获取有关当前时间的准确信息。NTP 服务是获取准确时间信息的一种方式，但此服务只能在所需防火墙端口打开的情况下运作。如果所有端口均处于关闭状态，此服务将无法实现其目标。NTP 服务提供一个选项，可配置启动或停止此服务的条件。此配置包括一些选项，指定是否打开防火墙端口，然后是否根据这些条件启动或停止 NTP 服务。有多个可能的配置选项，所有选项均同时适用于 SSH 服务器。

注意 本节中说明的设置仅适用于通过 vSphere Client 或借助于 vSphere Web Services SDK 创建的应用程序配置的服务设置。通过其他方式（例如 `esxcfg-firewall` 实用程序或 `/etc/init.d/` 中的配置文件）进行的配置不会受这些设置的影响。

- **如果任何端口打开则自动启动，如果所有端口关闭则停止** - 这是这些服务的默认设置，也是 Vmware 推荐的设置。如果任何端口打开，则客户端会尝试联系与相关服务有关的网络资源。如果某些端口已打开，但特定服务的端口已关闭，则该尝试将失败，但几乎不会对此类情况造成障碍。当适用的出站端口打开时，此服务将开始完成其任务。

- **与主机一起启动和停止** – 服务在主机启动后立即启动，并在主机关机之前不久关闭。此选项与**如果任何端口打开则自动启动，如果所有端口关闭则停止**非常相似，都意味着此服务定期尝试完成其任务（例如尝试连接指定的 NTP 服务器）。如果端口先是处于关闭状态，但随后又打开了，客户端将在此后不久开始完成其任务。

- **手动启动和停止** – 主机保留用户指定的服务设置，无论端口打开与否。当用户启动 NTP 服务后，只要主机仍然开启，该服务会一直运行。如果服务已启动且主机已关闭，该服务将在关机过程中停止，但是，主机一启动，该服务将再次启动，保留用户确定的状况。

配置服务启动与防火墙配置的关系

“启动策略”决定服务启动的条件。可以通过编辑“启动策略”来配置服务启动与防火墙配置的关系。

步骤

1 使用 vSphere Client 登录到 vCenter Server 系统。

2 在“清单”面板中选择主机。

3 依次单击**配置**选项卡和**安全配置文件**。

   vSphere Client 将显示与相应防火墙端口连接的入站和出站活动列表。

4 单击**属性**。

   “防火墙属性”对话框列出了可为主机配置的所有服务和管理代理。

5 选择要配置的服务，然后单击**选项**。

   “启动策略”对话框决定服务启动的条件。此对话框提供有关服务当前状况的信息，还提供手动启动、停止或重新启动服务的界面。

6 从**启动策略**列表中选择策略。

7 单击**确定**。

用于管理访问的 TCP 和 UDP 端口

vCenter Server、ESX 主机及其他网络组件是使用预定的 TCP 和 UDP 端口进行访问的。若要从防火墙外管理网络组件，可能需重新配置防火墙以允许在适当端口的访问。

表 12-1 列出了 TCP 和 UDP 端口以及每个端口的目的和类型。

除非另有指定，否则这些端口通过服务控制台接口建立连接。

表 12–1 TCP 和 UDP 端口

端口	用途	流量类型
22	SSH 服务器	入站 TCP
80	HTTP 访问。 默认的非安全 TCP Web 端口，通常与端口 443 一起用作从 Web 访问 ESX 网络的访问前端。端口 80 将流量重定向到 HTTPS 登陆页面（端口 443）。 从 Web 到 vSphere Web Access 的连接 WS 管理	入站 TCP
123	NTP 客户端	出站 UDP
427	CIM 客户端使用服务位置协议版本 2 (SLPv2) 查找 CIM 服务器。	入站和出站 UDP
443	HTTPS 访问 vCenter Server 对 ESX 主机的访问 默认 SSL Web 端口 vSphere Client 对 vCenter Server 的访问 vSphere Client 对 ESX 主机的访问 WS 管理 vSphere Client 对 vSphere Update Manager 的访问 vSphere Converter 对 vCenter Server 的访问 vSphere Web Access 和第三方网络管理客户端与 vCenter Server 的连接 vSphere Web Access 和第三方网络管理客户端对主机的直接访问	入站 TCP

表 12–1 TCP 和 UDP 端口 （续）

端口	用途	流量类型
902	主机对其他主机的访问以进行迁移和置备 ESX 的身份验证流量 (xinetd/vmware-authd) vSphere Client 对虚拟机控制台的访问 (UDP) 从 ESX 到 vCenter Server 的状态更新（检测信号）连接	入站 TCP，出站 UDP
903	用户在特定 ESX 主机上访问虚拟机时生成的远程控制台流量。 vSphere Client 对虚拟机控制台的访问 vSphere Web Access Client 对虚拟机控制台的访问 MKS 事务 (xinetd/vmware-authd-mks)	入站 TCP
2049	来自 NFS 存储设备的事务 此端口用于 VMkernel 接口，而不是服务控制台接口。	入站和出站 TCP
2050 – 2250	ESX 主机之间的流量，用于 VMware High Availability (HA) 和 EMC 自动启动管理器	出站 TCP，入站和出站 UDP
3260	到 iSCSI 存储设备的事务 此端口用于 VMkernel 接口和服务控制台接口。	出站 TCP
5900-5964	由 VNC 等管理工具使用的 RFB 协议	入站和出站 TCP
5989	通过 HTTPS 的 CIM XML 事务	入站和出站 TCP
8000	来自 vMotion 的请求 此端口用于 VMkernel 接口，而不是服务控制台接口。	入站和出站 TCP
8042 – 8045	ESX 主机之间的流量，用于 HA 和 EMC 自动启动管理器	出站 TCP，入站和出站 UDP
8100, 8200	ESX 主机之间的流量，用于 VMware 容错	出站 TCP，入站和出站 UDP

除 表 12–1 中所列的 TCP 和 UDP 端口外，还可根据需要配置其他端口：

- 可使用 vSphere Client 为已安装的管理代理和支持的服务（例如 NFS）打开端口。
- 可以通过运行命令行脚本在服务控制台防火墙中为网络所需的其他服务和代理打开端口。

通过 VLAN 确保虚拟机安全

网络可能是任何系统中最脆弱的环节之一。虚拟机网络需要的保护丝毫不应少于物理网络。可以通过多种方式加强虚拟机网络安全。

如果将虚拟机网络连接到物理网络，则其遭到破坏的风险不亚于由物理机组成的网络。即使虚拟机网络已与任何物理网络隔离，虚拟机也可能遭到网络中其他虚拟机的攻击。用于确保虚拟机安全的要求通常与物理机相同。

虚拟机是相互独立的。一个虚拟机无法读取或写入另一个虚拟机的内存、访问其数据、使用其应用程序等等。但在网络中，任何虚拟机或虚拟机组仍可能遭到其他虚拟机的未授权访问，因此可能需要通过外部手段加强保护。

可以通过不同方式增加这层保护：

- 为虚拟网络增加防火墙保护，方法是在其中的部分或所有虚拟机上安装和配置基于主机的防火墙。

为提高效率，可设置专用虚拟机以太网或虚拟网络。有了虚拟网络，可在网络最前面的虚拟机上安装基于主机的防火墙。这可以充当物理网络适配器和虚拟网络中剩余虚拟机之间的保护性缓存。

在虚拟网络最前面的虚拟机上安装基于主机的防火墙是一项不错的安全措施。但是，基于主机的防火墙会降低性能，因此请先对安全需求和性能进行权衡，然后再决定在虚拟网络中的其他虚拟机上安装基于主机的防火墙。

- 将主机中的不同虚拟机区域置于不同网络段上。如果将虚拟机区域隔离在自己的网络段中，可以大大降低虚拟机区域间泄漏数据的风险。分段可防止多种威胁，包括地址解析协议 (ARP) 欺骗，即攻击者操作 ARP 表以重新映射 MAC 和 IP 地址，从而访问进出主机的网络流量。攻击者使用 ARP 欺骗生成拒绝服务，劫持目标系统并以其他方式破坏虚拟网络。

  仔细计划分段可降低虚拟机区域间传输数据包的几率，从而防止嗅探攻击（此类攻击需向受害者发送网络流量）。此外，攻击者无法使用一个虚拟机区域中的不安全服务访问主机中的其他虚拟机区域。可以使用两种方法之一实施分段，每种方法具有不同优势。

  - 为虚拟机区域使用单独的物理网络适配器以确保将区域隔离。为虚拟机区域使用单独的物理网络适配器可能是最安全的方法，并且更不容易在初次创建段之后出现配置错误。
  - 设置虚拟局域网 (VLAN) 以帮助保护网络。VLAN 几乎能够提供以物理方式实施单独网络所具有的所有安全优势，但省去了硬件开销，可为您节省部署和维护附加设备、线缆等硬件的成本，是一种可行的解决方案。

VLAN 是一种 IEEE 标准的网络方案，通过特定的标记方法将数据包的传送限制在 VLAN 中的端口内。若配置正确，VLAN 将是您保护一组虚拟机免遭意外或恶意侵袭的可靠方法。

VLAN 可让您对物理网络进行分段，以便只有属于相同 VLAN 的网络中的两个虚拟机才能相互传输数据包。例如，会计记录和会计帐务是一家公司最敏感的内部信息。如果公司的销售、货运和会计员工均使用同一物理网络中的虚拟机，可按图 12-4 所示设置 VLAN 以保护会计部门的虚拟机。

图 12–4 VLAN 布局示例

在此配置中，会计部门的所有员工均使用 VLAN A 中的虚拟机，销售部门的员工使用 VLAN B 中的虚拟机。

路由器将包含会计数据的数据包转发至交换机。这些数据包将被标记为仅分发至 VLAN A。因此，数据将被局限在广播域 A 内，无法传送到广播域 B，除非对路由器进行此配置。

该 VLAN 配置可防止销售人员截取传至会计部门的数据包。还可防止会计部门接收传至销售组的数据包。一个虚拟交换机可为不同 VLAN 中的虚拟机服务。

VLAN 安全注意事项

如何设置 VLAN 以确保网络组件安全取决于客户机操作系统以及网络设备的配置方式。

ESX 配备完整的符合 IEEE 802.1q 的 VLAN 实施。VMware 不能对如何设置 VLAN 提出具体建议，但当您使用 VLAN 部署作为安全执行策略一部分时，应考虑以下因素。

将 VLAN 视作更广的安全实施的一部分

VLAN 能够有效地控制数据在网络中的传输位置和范围。如果攻击者可以访问网络，其攻击行为可能仅限于用作入口点的 VLAN，从而降低了攻击整个网络的风险。

VLAN 之所以能够提供保护，只是因为它可以控制数据在通过交换机并进入网络后的传送和包含方式。可使用 VLAN 以帮助确保网络架构的第 2 层（数据链接层）安全。但是，配置 VLAN 不能保护网络模型的物理层或任何其他层。即使创建 VLAN，也应通过确保硬件（路由器、集线器等等）安全和加密数据传输来提供额外保护。

VLAN 不能代替虚拟机配置中的防火墙。大多数包括 VLAN 的网络配置也同时包括防火墙。如果虚拟网络中包括 VLAN，请确保所安装的防火墙能够识别 VLAN。

正确配置 VLAN

设备配置错误及网络硬件、固件或软件缺陷会导致 VLAN 容易遭到 VLAN 跳转攻击。

如果有权访问一个 VLAN 的攻击者创建了一些数据包，并用欺骗手段致使物理交换机将这些数据包传输到其无权访问的另一个 VLAN，则将发生 VLAN 跳转。容易受到此类攻击的原因通常是由于对本机 VLAN 操作进行了错误的交换机配置，从而导致交换机可以接收和传输未标记数据包。

为帮助防止 VLAN 跳转，请及时安装硬件和固件更新以确保设备是最新的。同时请在配置设备时遵照供应商的最佳做法准则。

VMware 虚拟交换机不支持本机 VLAN 的概念。通过这些交换机的所有数据都会被适当地标记。但是，网络中可能有其他为本机 VLAN 操作配置的交换机，因此配置了虚拟交换机的 VLAN 仍然容易遭受 VLAN 跳转。

如果计划使用 VLAN 执行网络安全，则应对所有交换机禁用本机 VLAN 功能，除非必须在本机模式中操作某些 VLAN。如果必须使用本机 VLAN，请注意交换机供应商就此功能提供的配置准则。

在管理工具和服务控制台之间创建单独的通信

无论是使用管理客户端还是命令行，ESX 的所有配置任务均通过服务控制台来执行，这些任务包括配置存储器、控制虚拟机行为的各个方面及设置虚拟交换机或虚拟网络。由于服务控制台是 ESX 的控制点，因此确保其免遭误用非常关键。

VMware ESX 管理客户端使用身份验证和加密方法来防止对服务控制台进行未授权的访问，而其他服务可能不提供相同的保护。如果攻击者可以访问服务控制台，便可以随意地重新配置 ESX 主机的许多属性，例如更改整个虚拟交换机配置或更改授权方法。

服务控制台的网络连接通过虚拟交换机建立。要为这个关键的 ESX 组件提供更好的保护，可使用以下任一方法隔离服务控制台：

- 为管理工具与服务控制台之间的通信创建单独的 VLAN。
- 配置网络访问，以便通过一个虚拟交换机及一个或多个上行链路端口连接管理工具和服务控制台。

两种方法均可防止任何无法访问服务控制台 VLAN 或虚拟交换机的用户看到进出服务控制台的流量。还可防止攻击者向服务控制台发送数据包。您也可以选择在单独的物理网络段上配置服务控制台。物理分段可提供一层额外的安全保护，因为其后期更不容易出现配置错误。

为 vMotion 和网络附加存储设置单独的 VLAN 或虚拟交换机。

虚拟交换机保护和 VLAN

通过 VMware 虚拟交换机可阻止某些威胁 VLAN 安全的行为。虚拟交换机的设计方式使其可以防御各种攻击，其中多种攻击均涉及 VLAN 跳转。

有了这层保护并不能保证您的虚拟机配置不会遭受其他类型的攻击。例如，虚拟交换机只能保护虚拟网络免遭这些攻击，但不能保护物理网络。

虚拟交换机和 VLAN 可以抵御以下类型的攻击。

MAC 洪水

使交换机充满大量数据包，其中包含标记为来自不同源的 MAC 地址。许多交换机使用内容可寻址内存 (CAM) 表了解和存储每个数据包的源地址。当此表填满时，交换机可以进入完全打开状况，此时将在所有端口广播每个入站数据包，致使攻击者看到交换机的所有流量。此状况可能导致 VLAN 间的数据包泄漏。

尽管VMware虚拟交换机存储MAC地址表，但不会获取来自可观测流量的MAC地址，因此不容易受到此类攻击。

802.1q 和 ISL 标记攻击

强制交换机将帧从一个 VLAN 重定向至另一个 VLAN，方法是通过欺骗手段致使交换机充当中继并向其他 VLAN 广播流量。

VMware 虚拟交换机不执行此类攻击所需的动态中继，因此不会遭到攻击。

双重封装攻击

当攻击者创建一个双重封装数据包，其内部标记中的 VLAN 标识符与外部标记中的 VLAN 标识符不同时出现。为实现向后兼容性，本机 VLAN 将去除传输数据包的外部标记，除非进行其他配置。当本机 VLAN 交换机去除外部标记后，只剩下内部标记，它将把数据包路由到与所去除外部标记中标识的 VLAN 不同的 VLAN。

VMware 虚拟交换机会丢弃虚拟机尝试通过为特定 VLAN 配置的端口发送的任何双重封装帧。因此，它们不容易遭到此类攻击。

多播暴力攻击

涉及到将大量多播帧几乎同时发送到已知 VLAN，使交换机过载，从而错误地允许向其他 VLAN 广播一些帧。

VMware 虚拟交换机不允许帧离开其正确的广播域 (VLAN)，因此不容易遭到此类攻击。

跨树攻击

针对跨树协议 (STP)，此协议用于控制 LAN 组件间的桥接。攻击者发送网桥协议数据单元 (BPDU) 数据包，尝试更改网络拓扑，将攻击者自己建立成为根网桥。作为根网桥，攻击者可以嗅探传输帧的内容。

VMware 虚拟交换机不支持 STP，因此不容易遭到此类攻击。

随机帧攻击

涉及发送大量数据包，这些数据包的源地址和目标地址保持不变，但字段的长度、类型或内容会随机变化。此类攻击的目标是强制交换机错误地将数据包重新路由到不同 VLAN。

VMware 虚拟交换机不容易遭到此类攻击。

由于将来还会不断出现新的安全威胁，因此请勿将此视作有关攻击的详尽列表。请定期查看网站上的 VMware 安全资源，了解安全警示、近期安全警示及 VMware 安全策略。

确保虚拟交换机端口安全

与物理网络适配器一样，虚拟网络适配器也可以发送看上去来自不同计算机的帧或模拟另一台计算机，以便可以接收传至该计算机的网络帧。此外，虚拟网络适配器也可以像物理网络适配器一样进行配置以接收传至其他计算机的帧。

当您为网络创建虚拟交换机时，会添加端口组，为附加到交换机的虚拟机和存储系统强加策略配置。可通过 vSphere Client 创建虚拟端口。

在虚拟交换机中添加端口或端口组的过程中，vSphere Client 会为端口配置安全配置文件。此安全配置文件可用来确保 ESX 阻止其虚拟机的客户机操作系统模拟网络上的其他计算机。实施此安全功能的目的在于使负责模拟的客户机操作系统检测不到模拟行为已被阻止。

安全配置文件决定您对虚拟机执行的防模拟和截断攻击保护强度。为了正确使用安全配置文件中的设置，必须了解一些虚拟网络适配器如何控制传送及此级别的攻击如何进行的基础知识。

创建每个虚拟网络适配器时，都将向其分配自己的 MAC 地址。此地址称为初始 MAC 地址。尽管可以从客户机操作系统外部重新配置初始 MAC 地址，但不能由客户机操作系统进行更改。此外，每个适配器具有一个有效 MAC 地址，可筛选目标 MAC 地址与该有效 MAC 不同的入站网络流量。客户机操作系统负责设置有效 MAC 地址，并通常将有效 MAC 地址与初始 MAC 地址保持一致。

发送数据包时，操作系统通常将其网络适配器的有效 MAC 地址输入以太网帧的源 MAC 地址字段中。它还将接收网络适配器的 MAC 地址输入目标 MAC 地址字段。接收网络适配器仅在数据包的目标 MAC 地址与其自己的有效 MAC 地址匹配时才接受数据包。

网络适配器一经创建后，其有效 MAC 地址与初始 MAC 地址相同。虚拟机的操作系统可随时将有效 MAC 地址更改为其他值。如果操作系统更改了有效 MAC 地址，其网络适配器将接收传至新 MAC 地址的网络流量。操作系统可随时发送带有模拟源 MAC 地址的帧。这意味着操作系统便可通过模拟接收网络授权的网络适配器对网络中的设备进行恶意攻击。

可以使用 ESX 主机上的虚拟交换机安全配置文件设置三个选项以防止此类攻击。如果更改端口的任何默认设置，必须在 vSphere Client 中通过编辑虚拟交换机设置来修改安全配置文件。

MAC 地址更改

MAC 地址更改选项的设置将影响虚拟机接收的流量。

当此选项设置为**接受**时，ESX 主机接受将有效 MAC 地址更改为非初始 MAC 地址的请求。

当选项设置为**拒绝**时，ESX 不接受将有效 MAC 地址更改为非初始 MAC 地址的请求，这会保护主机免受 MAC 模拟。虚拟适配器用于发送请求的端口将被禁用，必须在它将有效 MAC 地址更改为初始 MAC 地址后才能再接收帧。客户机操作系统检测不到 MAC 地址更改已被拒绝。

注意 iSCSI 启动器依赖于能够从某些类型的存储器获取 MAC 地址更改。如果使用 ESX iSCSI，并且有 iSCSI 存储器，则将 **MAC 地址更改**选项设置为**接受**。

有时您可能确实需要多个适配器在网络中使用同一 MAC 地址（例如在单播模式中使用 Microsoft 网络负载平衡时）。在标准多播模式下使用 Microsoft 网络负载平衡时，适配器不能共享 MAC 地址。

伪信号

伪信号选项的设置将影响从虚拟机传输的流量。

当选项设置为**接受**时，ESX 不会比较源 MAC 地址和有效 MAC 地址。

要防止MAC模拟，可将此选项设置为**拒绝**。这样，主机将对操作系统传输的源MAC地址与其适配器的有效MAC地址进行比较，以确认是否匹配。如果地址不匹配，ESX 将丢弃数据包。

客户机操作系统检测不到其虚拟网络适配器无法使用模拟 MAC 地址发送数据包。ESX 主机会在带有模拟地址的任何数据包递送之前将其截断，而客户机操作系统可能假设数据包已被丢弃。

杂乱模式运行

杂乱模式会清除虚拟网络适配器执行的任何接收筛选，以便客户机操作系统接收在网络上观察到的所有流量。默认情况下，虚拟网络适配器不能在杂乱模式中运行。

尽管杂乱模式对于跟踪网络活动很有用，但它是一种不安全的运行模式，因为杂乱模式中的任何适配器均可访问数据包，而与某些数据包是否仅由特定的网络适配器接收无关。这意味着虚拟机中的管理员或 root 用户可以查看发往其他客户机或主机操作系统的流量。

注意 有时您可能确实需要将虚拟交换机配置为在杂乱模式中运行（例如运行网络入侵检测软件或数据包嗅探器时）。

Internet 协议安全

Internet 协议安全 (IPsec) 用于确保进出主机的 IP 通信安全。ESX 主机支持使用 IPv6 的 IPsec。

在主机上设置 IPsec 时，可对入站和出站数据包启用身份验证和加密。对 IP 流量进行加密的时间和方式取决于如何设置系统的安全关联和安全策略。

安全关联确定系统对流量进行加密的方式。在创建安全关联时，可指定安全关联的源和目标、加密参数和名称。

安全策略确定系统应对流量进行加密的时间。安全策略包括源和目标信息、要加密的流量的协议和方向、模式（transport 或 tunnel）以及要使用的安全关联。

服务控制台上基于 IPv6 的 IPsec 不受支持。

添加安全关联

添加安全关联以指定关联的 IP 流量的加密参数。

可以使用 vSphere CLI 添加安全关联。有关使用 vSphere CLI 的信息，请参见《vSphere 命令行界面安装和脚本指南》和《vSphere 命令行界面参考》。

步骤

1 使用命令 `esxcfg-ipsec --add-sa`。

2 使用 `--sa-src` 源地址指定源地址。

3 使用 `--sa-dst` 目标地址指定目标地址。

4 使用 `--sa-mode` 模式选择模式（`transport` 或 `tunnel`）。

5 使用 `--spi` 安全参数索引提供安全参数索引。

   安全参数索引标识与主机的安全关联。它必须是一个十六进制数并带有 0x 前缀。所创建的每个安全关联都必须具有协议和安全参数索引的唯一组合。

6 使用 `--ealgo` 加密算法选择加密算法。

   - `3des-cbc`
   - `aes128-cbc`
   - `null` 不提供任何加密

7 使用 `--ekey` 加密密钥提供加密密钥。

   可以使用 0x 前缀输入 ASCII 文本或十六进制形式的密钥。

8 使用 `--ialgo` 身份验证算法选择身份验证算法（`hmac-sha1` 或 `hmac-sha2-256`）。

9 使用 `--ikey` 身份验证密钥提供身份验证密钥。

   可以使用 0x 前缀输入 ASCII 文本或十六进制形式的密钥。

10 使用 `name` 提供安全关联的名称。

示例 12–1 新安全关联命令示例

为了方便阅读，下面的示例包含额外的换行符。

```
esxcfg-ipsec --add-sa
--sa-src 3ffe:501:ffff:0::a
--sa-dst 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--spi 0x1000
--ealgo 3des-cbc
--ekey 0x6970763672656164796c6f676f336465736362636f757432
--ialgo hmac-sha1
--ikey 0x6970763672656164796c6f67736861316f757432
sa1
```

移除安全关联

可以从 ESX 主机中移除安全关联。

可以使用 vSphere CLI 移除安全关联。有关使用 vSphere CLI 的信息，请参见《vSphere 命令行界面安装和脚本指南》和《vSphere 命令行界面参考》。

前提条件

请确保要使用的安全关联当前未在使用。如果尝试移除正在使用中的安全关联，则移除操作将失败。

步骤

◆ 使用命令 `esxcfg-ipsec --remove-sa` 安全关联名称。

列出可用的安全关联

ESX 可提供可供安全策略使用的所有安全关联的列表。该列表包含用户创建的安全关联，以及 VMkernel 使用 Internet 密钥交换安装的任何安全关联。

可以使用 vSphere CLI 获得可用安全关联的列表。有关使用 vSphere CLI 的信息，请参见《vSphere 命令行界面安装和脚本指南》和《vSphere 命令行界面参考》。

步骤

◆ 使用命令 `esxcfg-ipsec -l`。

ESX 将显示所有可用安全关联的列表。

创建安全策略

创建安全策略可以确定何时使用在安全关联中设置的身份验证和加密参数。

可以使用 vSphere CLI 添加安全策略。有关使用 vSphere CLI 的信息，请参见《vSphere 命令行界面安装和脚本指南》和《vSphere 命令行界面参考》。

前提条件

在创建安全策略之前，可添加具有相应身份验证和加密参数的安全关联。

步骤

1 使用命令 `esxcfg-ipsec --add-sp`。
2 使用 `--sp-src` 源地址指定源 IP 地址和前缀长度。
3 使用 `--sp-dst` 目标地址指定目标地址和前缀长度。
4 使用 `--src-port` 端口指定源端口。

   源端口号必须是介于 0 和 65535 之间的一个数字。

5 使用 `--dst-port` 端口指定目标端口。

   目标端口号必须是介于 0 和 65535 之间的一个数字。

6 使用 `--ulproto` 协议选择上层协议。
   - `tcp`
   - `udp`
   - `icmp6`
   - `any`
7 选择方向（`in` 或 `out`），您要使用 `--dir` 方向监视该方向的流量。
8 使用 `--action` 操作指定在遇到具有指定参数的流量时要采取的操作。

选项	描述
无	不采取任何操作。
discard	不允许数据进出。
ipsec	使用安全关联中提供的身份验证和加密信息来确定数据是否来自受信任的源。

9 使用 `--sp-mode` 模式选择模式（`transport` 或 `tunnel`）。
10 使用 `--sa-name` 安全关联名称为此要使用的安全策略指定安全关联。
11 使用 `name` 指定安全策略的名称。

示例 12-2 新安全策略命令示例

为了方便阅读，下面的示例包含额外的换行符。

```
esxcfg-ipsec --add-sp
--sp-src 2001:db8:1::/64
--sp-dst 2002:db8:1::/64
--src-port 23
--dst-port 25
--ulproto tcp
--dir out
--action ipsec
--sp-mode transport
--sa-name sa1
sp1
```

移除安全策略

可以从 ESX 主机中移除安全策略。

可以使用 vSphere CLI 移除安全策略。有关使用 vSphere CLI 的信息，请参见《vSphere 命令行界面安装和脚本指南》和《vSphere 命令行界面参考》。

前提条件

请确保要使用的安全策略当前未在使用。如果尝试移除正在使用中的安全策略，则移除操作将失败。

步骤

◆ 使用命令 `esxcfg-ipsec --remove-sp` 安全策略名称。

列出可用的安全策略

ESX 可以提供主机上所有安全策略的列表。

可以使用 vSphere CLI 获得可用安全策略的列表。有关使用 vSphere CLI 的信息，请参见《vSphere 命令行界面安装和脚本指南》和《vSphere 命令行界面参考》。

步骤

◆ 使用命令 `esxcfg-ipsec -L`。

ESX 将显示所有可用安全策略的列表。

确保 iSCSI 存储器安全

为 ESX 主机配置的存储器可能包括一个或多个使用 iSCSI 的存储区域网络 (SAN)。在 ESX 主机上配置 iSCSI 时，可采取几种措施降低安全风险。

iSCSI 是一种使用 TCP/IP 协议通过网络端口（而不是通过直接连接 SCSI 设备）来访问 SCSI 设备和交换数据记录的方法。在 iSCSI 事务中，原始 SCSI 数据块被封装在 iSCSI 记录中并传输至请求数据的设备或用户。

iSCSI SAN 可让您有效地利用现有以太网架构，为 ESX 主机提供对可供其动态共享的存储资源的访问。iSCSI SAN 可为依赖公用存储池为多个用户提供服务的环境提供经济的存储解决方案。与任何网络系统一样，iSCSI SAN 也可能遭到安全破坏。

注意 用于确保 iSCSI SAN 安全的要求和过程与可用于 ESX 主机的 iSCSI 硬件适配器和通过 ESX 主机直接配置的 iSCSI 相同。

通过身份验证确保 iSCSI 设备的安全

确保 iSCSI 免遭不利入侵的一种方法就是，每当主机尝试访问目标 LUN 上的数据时都要求 iSCSI 设备（或称目标）对 ESX 主机（或称启动器）进行身份验证。

身份验证的目的是证明启动器具有访问目标的权利，这是在您配置身份验证时授予的权利。

ESX 不支持 iSCSI 的 Kerberos、安全远程协议 (SRP) 或公用密钥身份验证方法。此外，它也不支持 IPsec 身份验证和加密。

使用 vSphere Client 可以确定当前是否在执行身份验证并配置身份验证方法。

为 iSCSI SAN 启用挑战握手身份验证协议 (CHAP)

可将 iSCSI SAN 配置为使用 CHAP 身份验证。

在 CHAP 身份验证中，当启动器联系 iSCSI 目标时，目标向启动器发送一个预定义 ID 值和一个随机值（或称键）。启动器创建一个单向哈希值，并将其发送给目标。此哈希值包含三个元素：目标发送的预定义 ID 值、随机值和一个由启动器和目标共享的专用值（或称 CHAP 密钥）。当目标收到启动器的哈希值后，将使用相同的元素创建自己的哈希值并将其与启动器的哈希值进行比较。如果结果匹配，目标将对启动器进行身份验证。

ESX 支持对 iSCSI 的单向和双向 CHAP 身份验证。在单向 CHAP 身份验证中，目标需验证启动器，但启动器无需验证目标。在双向 CHAP 身份验证中，提供了供启动器验证目标的附加安全级别。

当只有一组身份验证凭据可以从 ESX 主机发送到所有目标时，ESX 支持适配器级别的 CHAP 身份验证。还支持每个目标的 CHAP 身份验证，后者可让您为每个目标配置不同凭据以实现更好的目标优化。

有关如何处理 CHAP 的信息，请参见第 94 页，“配置 iSCSI 适配器的 CHAP 参数”。

禁用 iSCSI SAN 身份验证

可将 iSCSI SAN 配置为不使用身份验证。启动器与目标间的通信仍需经过初步身份验证，因为 iSCSI 目标设备通常会设置为仅与特定启动器通信。

如果您的 iSCSI 存储器位于一个位置且创建专用网络或 VLAN 为所有 iSCSI 设备提供服务，那么选择不执行更严格的身份验证可能有意义。iSCSI 配置是安全的，因为它与任何有害访问隔离，这与光纤通道 SAN 很相似。

通常，除非您愿意冒 iSCSI SAN 被攻击的风险，或需处理因人为错误而造成的问题，否则请勿禁用身份验证。

有关如何处理 CHAP 的信息，请参见第 94 页，“配置 iSCSI 适配器的 CHAP 参数”。

保护 iSCSI SAN

计划 iSCSI 配置时，应采取一些措施提高 iSCSI SAN 的整体安全。iSCSI 配置是否安全取决于 IP 网络，因此在设置网络时执行良好的安全标准可帮助保护 iSCSI 存储器。

下面是执行良好安全标准的一些具体建议。

保护传输数据

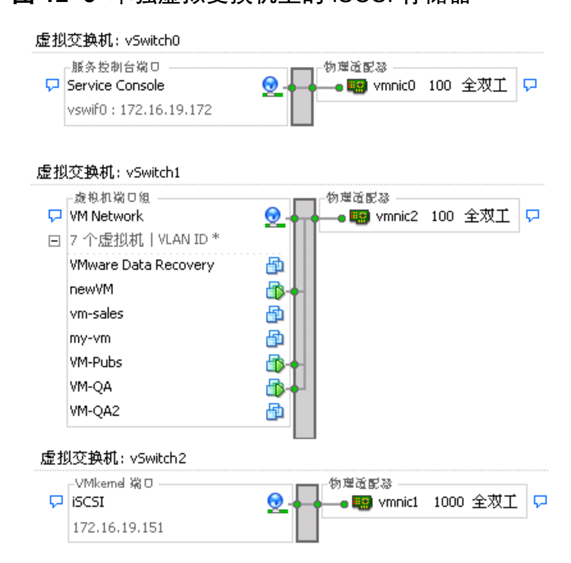
iSCSI SAN 中的一个主要安全风险便是攻击者会嗅探传输的存储数据。

采取其他措施以防止攻击者能够轻易看见 iSCSI 数据。无论是 iSCSI 硬件适配器还是 ESX 主机 iSCSI 启动器，均不会对其传输至目标和从目标接收的数据进行加密，这会造成数据更易遭到嗅探攻击。

通过 iSCSI 配置允许虚拟机共享虚拟交换机和 VLAN 可能导致 iSCSI 流量遭到虚拟机攻击者误用。为帮助确保入侵者无法侦听 iSCSI 传送数据，请确保任何虚拟机都无法看到 iSCSI 存储网络。

如果使用的是 iSCSI 硬件适配器，则可以通过以下操作来实现这一目的：确保 iSCSI 适配器和 ESX 物理网络适配器没有因共享交换机或某种其他方式而无意地在主机外部连接。如果直接通过 ESX 主机配置 iSCSI，可通过虚拟机未使用的另一个虚拟交换机来配置 iSCSI 存储器，如图 12-5 中所示。

图 12–5 单独虚拟交换机上的 iSCSI 存储器



除了通过提供专用虚拟交换机来保护 iSCSI SAN 外，还可以在 iSCSI SAN 自己的 VLAN 上对其进行配置以提高性能和安全性。将 iSCSI 配置放在单独的 VLAN 上可确保只有 iSCSI 适配器可以看到 iSCSI SAN 内的传送数据。此外，来自其他来源的网络拥堵不会影响 iSCSI 流量。

保护 iSCSI 端口安全

当运行 iSCSI 设备时，ESX 主机不会打开任何侦听网络连接的端口。此措施可降低入侵者通过空闲端口侵入 ESX 主机并控制主机的几率。因此，运行 iSCSI 不会在连接的 ESX 主机端产生任何额外安全风险。

您运行的任何 iSCSI 目标设备都必须具有一个或多个打开的 TCP 端口以侦听 iSCSI 连接。如果 iSCSI 设备软件中存在任何安全漏洞，则数据遭遇的风险并非 ESX 所造成。要降低此风险，请安装存储设备制造商提供的所有安全修补程序并对连接 iSCSI 网络的设备进行限制。

身份验证和用户管理 13

ESX 处理用户身份验证，并支持用户和组权限。此外，可以加密与 vSphere Client 和 SDK 的连接。

本章讨论了以下主题：

通过身份验证和权限确保 ESX 的安全

当 vSphere Client 或 vCenter Server 用户连接到 ESX 主机时，即会通过 VMware Host Agent 进程建立连接。该进程使用用户名和密码来进行验证。

ESX 使用“可插入认证模块 (PAM)”结构对使用 vSphere Client、vSphere Web Access 或服务控制台访问 ESX 主机的用户进行身份验证。VMware 服务的 PAM 配置位于 `/etc/pam.d/vmware-authd`，其中存储了身份验证模块的路径。

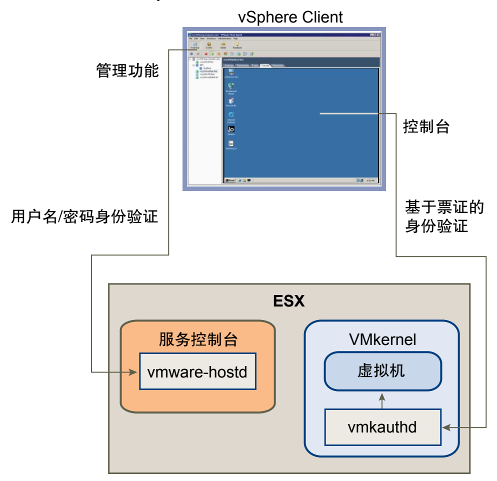
如同 Linux 一样，ESX 的默认安装使用 `/etc/passwd` 身份验证，但可对 ESX 进行配置以使用另一个分布式身份验证机制。如果要使用第三方身份验证工具，而不使用 ESX 默认实施，请参考供应商文档以查看说明。在设置第三方身份验证的过程中，可能需要使用新的模块信息来更新 `/etc/pam.d` 文件夹中的文件。

VMware 主机代理中的反向代理 (`vmware-hostd`) 进程侦听端口 80 和 443。vSphere Client 或 vCenter Server 用户通过这些端口连接到主机代理。`vmware-hostd` 进程从客户端接收用户名和密码，并将它们转发至 PAM 模块以执行身份验证。

图 13-1 说明了 ESX 如何从 vSphere Client 对事务进行身份验证的一个基本示例。

注意 在与 `vmware-hostd` 进程连接时，CIM 事务还使用基于票证的身份验证。

图 13–1 对 vSphere Client 与 ESX 之间的通信进行身份验证



通过 vSphere Web Access 和第三方网络管理客户端进行的 ESX 身份验证事务也会与 `vmware-hostd` 进程直接进行交互。

为了确保网站的身份验证能够高效工作，可执行一些基本任务，例如，设置用户、组、权限和角色；配置用户属性；添加自己的证书；确定是否要使用 SSL 等。

关于用户、组、权限和角色

vCenter Server 和 ESX 主机使用用户名、密码和权限的组合来验证用户访问权限，并对活动进行授权。通过分配权限，可以控制对主机、群集、数据存储、资源池、网络端口组和虚拟机的访问权限。

当具有适当权限的已知用户使用正确的密码登录主机时，系统会授予其对 ESX 主机及其资源的访问权限。当确定是否对用户授予访问权限时，vCenter Server 也使用类似方法。

vCenter Server 和 ESX 主机在下列情况下拒绝授予访问权限：

- 非用户列表上的用户尝试登录。
- 用户输入的密码不正确。
- 用户在列表上但未分配有权限。
- 已成功登录的用户尝试执行其不具有相应权限的操作。

在管理 ESX 主机和 vCenter Server 的过程中，您必须计划如何处理特定类型的用户和权限。ESX 和 vCenter Server 使用一组特权或角色来控制每个用户或组可执行的操作。系统提供了预定义的角色，但还可以创建新角色。分配给组的用户更易于管理。在将角色应用到组时，组中的所有用户将继承该角色。

本节中的主题适用于本地用户和组。此外，也可以使用 Active Directory 来管理 ESX 的用户和组。

了解用户

用户是经过授权可登录 ESX 主机或 vCenter Server 的个人。

ESX 用户分为两类：可通过 vCenter Server 访问主机的用户，以及通过从 vSphere Client、vSphere Web Access、第三方客户端或 Command Shell 直接登录主机来访问主机的用户。

vCenter Server 授权用户　　vCenter Server 授权用户包括在 vCenter Server 所引用的 Windows 域列表中，或者是 vCenter Server 主机上的本地 Windows 用户。

不能使用 vCenter Server 手动创建、移除或以其他方式更改用户。必须使用工具来管理 Windows 域。所作的任何更改将在 vCenter Server 中反映出来。但是，用户界面不提供用于检查的用户列表。

直接访问用户

经授权直接在 ESX 主机上工作的用户是系统管理员添加到内部用户列表的用户。

管理员可以对这些用户执行各种管理操作，如更改密码、组成员资格和权限以及添加和移除用户。

ESX 本地维护的用户列表与 vCenter Server 已知的用户是分开的，vCenter Server 已知的用户要么是本地 Windows 用户，要么是属于 Windows 域的用户。即使列表中似乎包含常见用户（例如，名为 devuser 的用户），也单独处理这些用户。如果以 devuser 用户身份登录 vCenter Server，则可能具有从数据存储查看和删除文件的权限，但是，如果以 devuser 用户身份登录 ESX 主机，则不具有这样的权限。如果主机上配置了活动目录身份验证，则 vCenter Server 已知的那些 Windows 域用户将在 ESX 主机上可用。

由于名称重复可能造成混乱，应在创建 ESX 主机用户之前对 vCenter Server 用户列表进行检查，以避免名称重复。要检查 vCenter Server 用户，请查看 Windows 域列表。

了解组

组是一组共享公用的规则和权限集的用户。向某个组分配权限时，该组中的所有用户都将继承这些权限，而不必逐个处理用户配置文件。

管理员需要决定如何建立组结构，以达到安全和使用目标。例如，三位兼职销售小组成员的工作时间各不相同，您希望他们共享一个虚拟机但不想让他们使用销售经理的虚拟机。在这种情况下，可以创建一个名为 SalesShare 的组，该组包括三个销售人员，并授予仅与一个对象（即共享虚拟机）进行交互的组权限。他们不能在销售经理的虚拟机上执行任何操作。

vCenter Server 和 ESX 主机中组列表的来源与其各自用户列表的来源相同。vCenter Server 中的组列表源自本地用户或任何信任域，ESX 主机的组列表源自本地用户列表或任何受信任的 Windows 域。

了解密码要求

默认情况下，ESX 强制执行用户密码相关要求。

在创建密码时，应包含以下四类字符的组合：小写字母、大写字母、数字和特殊字符（如下划线或短划线）。

用户密码必须满足以下长度要求。

- 包含一类或两类字符的密码的长度必须至少为八个字符。
- 包含三类字符的密码的长度必须至少为七个字符。
- 包含全部四类字符的密码的长度必须至少为六个字符。

注意 密码开头的大写字母不算入使用的字符类别数。密码结尾的数字不算入使用的字符类别数。

还可以使用至少包含三个单词且每个单词有 8 到 40 个字符的密码短语。

示例 13–1 密码示例

下列候选密码满足 ESX 的要求。

- xQaTEhbU:包含由两类字符组成的八个字符。
- xQaT3pb:包含由三类字符组成的七个字符。
- xQaT3#:包含由四类字符组成的六个字符。

下列候选密码不满足 ESX 的要求。

- Xqat3hb:以大写字符开头，可将有效字符种类数减少到两种。仅使用两种字符类别时，需要 8 个字符。
- xQaTEh2:以数字结尾，可将有效字符种类数减少到两种。仅使用两种字符类别时，需要 8 个字符。

了解权限

对于 ESX 和 vCenter Server，将权限定义为访问角色，访问角色由用户以及为对象（如虚拟机或 ESX 主机）分配的用户角色组成。

大多数 vCenter Server 和 ESX 用户对于与主机相关联的对象的操作能力很有限。具有管理员角色的用户对所有虚拟对象（如数据存储、主机、虚拟机和资源池）拥有完全访问权利和权限。默认情况下，向 root 用户授予管理员角色。如果主机由 vCenter Server 管理，则 vpxuser 也是管理员用户。

ESX 和 vCenter Server 的特权列表相同，您可以使用相同方法配置权限。

可通过直接连接到 ESX 主机来创建角色并设置权限。由于这些任务在 vCenter Server 中更广泛地执行，因此请参见《VMware vSphere 数据中心管理指南》获得有关处理权限和角色的信息。

分配 root 用户权限

root 用户只能在其登录的特定 ESX 主机上执行操作。

为安全起见，您可能不想以管理员角色使用 root 用户。在此情况下，可在安装后更改权限，以便使 root 用户不再拥有管理特权，也可通过 vSphere Client 一次性删除 root 用户的访问权限，如《VMware vSphere 数据中心管理指南》中所述。如果执行了此操作，必须首先在 root 级别创建可向另一个用户分配管理员角色的另一种权限。

向另一个用户分配管理员角色有助于通过可跟踪性维护安全。vSphere Client 将管理员角色用户启动的所有操作记录为事件，并为您提供审核记录。如果所有管理员均以 root 用户身份登录主机，则不能分辨某项操作是哪个管理员执行的。如果在 root 级别创建了多个权限，而且每个权限均与不同的用户或用户组相关联，则可对每个管理员或管理组的操作进行跟踪。

创建备用管理员用户后，就可以向 root 用户分配不同的角色。要使用 vCenter Server 管理主机，您创建的新用户必须对主机拥有完全管理员特权。

注意 `vicfg` 命令不执行访问检查。因此，即使限制 root 用户的特权，也不会影响用户可使用命令行界面命令执行的操作。

了解 vpxuser 权限

当 vCenter Server 管理主机活动时，它使用 vpxuser 权限。vpxuser 在将 ESX 主机连接到 vCenter Server 时创建。

vCenter Server 对其管理的主机拥有管理员特权。例如，vCenter Server 可将虚拟机移至和移离主机，并执行支持虚拟机所必需的配置更改。

vCenter Server 管理员可在主机上执行可以由 root 用户执行的大多数任务，并调度任务和处理模板等。但是，vCenter Server 管理员不能为 ESX 主机直接创建、删除或编辑用户和组。这些任务只能由具有管理员权限的用户直接在每台 ESX 主机上执行。

注意 不能使用 Active Directory 管理 vpxuser。



小心 不要以任何方式更改 vpxuser 及其权限。如果进行了更改，在通过 vCenter Server 处理 ESX 主机时可能会出现问题。

了解角色

vCenter Server 和 ESX 仅将对象的访问权限授予已针对该对象分配了权限的用户。向用户或组分配与对象相关的权限时，可通过将用户或组与角色进行配对来操作。角色是一组预定义的特权。

ESX 主机可提供三种默认的角色，您不能更改与这些角色相关联的特权。每个后续的默认角色均包括前一个角色的特权。例如，管理员角色继承只读角色的特权。您本人创建的角色不继承任何默认角色的特权。

可使用 vSphere Client 中的角色编辑功能创建自定义角色，以创建符合用户需求的特权组。如果使用与 vCenter Server 相连的 vSphere Client 来管理 ESX 主机，则可在 vCenter Server 中选择其他角色。同样，在 vCenter Server 中无法访问在 ESX 主机上直接创建的角色。仅当您直接从 vSphere Client 登录主机时，才可使用这些角色。

如果通过 vCenter Server 管理 ESX 主机，则在主机和 vCenter Server 中维护自定义角色可能会引起混淆和误用。在此类型配置中，应仅在 vCenter Server 中维护自定义角色。

可通过直接连接到 ESX 主机来创建角色并设置权限。由于大多数用户在 vCenter Server 中创建角色并设置权限，因此请参见《VMware vSphere 数据中心管理指南》获取有关处理权限和角色的信息。

分配无权访问角色

分配有无权访问角色的对象用户不能以任何方式查看或更改对象。默认情况下向新用户和组分配此角色。可以逐对象更改角色。

默认情况下，root 用户和 vpxuser 权限是未分配有无权访问角色的唯一用户。相反，它们分配有管理员角色。只要首先在 root 级别使用管理员角色创建替代权限并将此角色与另一个用户相关联，就可以完全删除 root 用户的权限或将其角色更改为无权访问。

分配只读角色

分配有只读角色的对象用户可查看对象的状况和详细信息。

具有此角色的用户可查看虚拟机、主机和资源池属性。该用户不能查看主机的远程控制台。通过菜单和工具栏执行的所有操作均被禁止。

分配管理员角色

分配有管理员角色的对象用户可在对象上查看和执行所有操作。此角色也包括只读角色固有的所有权限。

如果以管理员角色在 ESX 主机上执行操作，则可向该主机上的每个用户和组授予权限。如果以管理员角色在 vCenter Server 中执行操作，则可向 vCenter Server 引用的 Windows 域列表中包括的任何用户或组授予权限。

vCenter Server 通过分配权限这一过程对选定的任何 Windows 域用户或组进行注册。默认情况下，向属于 vCenter Server 上本地 Windows Administrators 组的所有用户授予与分配至管理员角色的任何用户相同的访问权限。属于 Administrators 组的用户可以以个人身份登录并具有完全访问权限。

属于活动目录组 ESX Admins 的用户将自动分配有管理员角色。

为安全起见，可考虑从管理员角色中移除 Windows Administrators 组。可以在安装之后更改权限。此外，可以使用 vSphere Client 删除 Windows Administrators 组访问权限，但必须首先在 root 级别创建可向另一个用户分配管理员角色的另一种权限。

处理 ESX 主机上的用户和组

如果通过 vSphere Client 直接连接 ESX 主机，则可创建、编辑和删除用户和组。只要登录 ESX 主机，就会在 vSphere Client 中看到这些用户和组，但在登录 vCenter Server 时看不见。

本节中的主题适用于本地用户和组。此外，也可以使用 Active Directory 来管理 ESX 的用户和组。

查看和导出用户和组列表并对其进行排序

可以查看 ESX 用户和组的列表，对其进行排序，并将其导出到 HTML、XML、Microsoft Excel 或 CSV 格式的文件中。

步骤

1 通过 vSphere Client 登录主机。

2 单击**用户和组**选项卡，然后单击**用户**或**组**。

3 根据希望在导出文件中看到的信息，确定如何对表进行排序以及如何隐藏或显示列。

- 要按任意列对表进行排序，请单击列标题。
- 要显示或隐藏列，请右键单击任何列标题，并选择或取消选择要隐藏的列的名称。
- 要显示或隐藏列，请右键单击任何列标题，并选择或取消选择要隐藏的列的名称。

4 右键单击表中的任何位置，然后单击**导出列表**以打开“另存为”对话框。

5 选择路径并输入文件名。

6 选择文件类型，然后单击**确定**。

将用户添加到用户表

将用户添加到用户表会更新由 ESX 维护的内部用户列表。

前提条件

查看第 157 页，“了解密码要求”中所述的密码要求。

步骤

1 通过 vSphere Client 登录主机。

2 单击**用户和组**选项卡，然后单击**用户**。

3 右键单击“用户”表中的任何位置，然后单击**添加**以打开“新增用户”对话框。

4 输入登录名、用户名、数字用户 ID (UID) 和密码。

- 对于用户名和 UID 的指定是可选操作。如果未指定 UID，vSphere Client 将分配下一个可用的 UID。
- 创建符合长度和复杂性要求的密码。主机将使用默认身份验证插件 `pam_passwdqc.so` 来检查密码合规性。如果密码不合规，将显示以下错误：发生了一般系统错误：密码：身份验证标记操作错误。
- 如果切换到 `pam_cracklib.so` 身份验证插件，将不强制执行密码合规性。

5 要允许用户通过 Command Shell 访问 ESX 主机，请选择**授于该用户 shell 程序访问权限**。

注意 要想获得 shell 访问权限，用户还必须对主机上的清单对象具有管理员角色。

通常，不要向用户授予 shell 访问权限，除非确定其有必要通过 shell 访问主机。仅通过 vSphere Client 访问主机的用户不需要具有 Shell 访问权限。

6 要将用户添加到组，请从**组**下拉菜单选择组名称，然后单击**添加**。

7 单击**确定**。

修改用户设置

可以更改用户的用户 ID、用户名、密码和组设置。还可以向用户授予 shell 访问权限。

前提条件

查看第 157 页，“了解密码要求”中所述的密码要求。

步骤

1 通过 vSphere Client 登录主机。

2 单击**用户和组**选项卡，然后单击**用户**。

3 右键单击用户，然后单击**编辑**以打开“编辑用户”对话框。

4 要更改用户 ID，请在 **UID** 文本框中输入数值用户 ID。

   vSphere Client 在您首次创建用户时分配 UID。在大多数情况下，可以不更改此分配。

5 请输入新的用户名。

6 要更改用户密码，请选择**更改密码**，然后输入新密码。

   ■ 创建符合长度和复杂性要求的密码。主机将使用默认身份验证插件 `pam_passwdqc.so` 来检查密码合规性。如果密码不合规，将显示以下错误：发生了一般系统错误：密码：身份验证标记操作错误。

   ■ 如果切换到 `pam_cracklib.so` 身份验证插件，将不强制执行密码合规性。

7 要更改用户通过 Command Shell 访问 ESX 主机的能力，请选择或取消选择**授于该用户 shell 程序访问权限**。

   注意 要想获得 shell 访问权限，用户还必须对主机上的清单对象具有管理员角色。

   通常，不要向用户授予 shell 访问权限，除非确定其有必要通过 shell 访问主机。仅通过 vSphere Client 访问主机的用户不需要具有 Shell 访问权限。

8 要将用户添加到组，请从**组**下拉菜单选择组名称，然后单击**添加**。

9 要从某个组中移除用户，请从**组成员资格**框中选择该组的名称，然后单击**移除**。

10 单击**确定**。

移除用户或组

可以从 ESX 主机中移除用户或组。



小心 不要移除 root 用户。

如果从主机中移除用户，其将失去对主机中所有对象的权限，且无法再次登录。

注意 如果从域中移除已登录的用户，其主机权限在您重新启动主机前将予以保留。

移除组并不会影响单独授予该组中用户的权限，也不会影响作为另一个组的部分包含项授予的权限。

步骤

1 通过 vSphere Client 登录主机。
2 单击**用户和组**选项卡，然后单击**用户**或**组**。
3 右键单击要移除的用户或组，然后单击**移除**。

将组添加到组表

将组添加到 ESX 组表会更新由主机维护的内部组列表。

步骤

1 通过 vSphere Client 登录主机。
2 单击**用户和组**选项卡，然后单击**组**。
3 右键单击“组”表中的任何位置，然后单击**添加**以打开“创建新组”对话框。
4 在**组 ID** 字段中输入组名称和数值组 ID (GID)。

   对于 GID 的指定是可选的。如果未指定 GID，vSphere Client 将分配下一个可用的组 ID。
5 对于要添加为组成员的每个用户，从列表中选择用户名，然后单击**添加**。
6 单击**确定**。

添加或移除组中的用户

可以向组表的组中添加用户或从中移除用户。

步骤

1 通过 vSphere Client 登录主机。
2 单击**用户和组**选项卡，然后单击**组**。
3 右键单击要修改的组，然后单击**属性**以打开“编辑组”对话框。
4 要将用户添加到组，请从**组**下拉菜单选择组名称，然后单击**添加**。
5 要从某个组中移除用户，请从**组成员资格**框中选择该组的名称，然后单击**移除**。
6 单击**确定**。

配置主机以使用目录服务

可配置 ESX 主机，以便使用目录服务（如活动目录）来管理用户和组。

前提条件

确认您已设置活动目录域。请参见目录服务器文档。

步骤

1 确保 ESX 的主机名完全符合活动目录林的域名条件。

全限定域名 = 主机名.域名

2 使用您的首选方法将 ESX 和目录服务系统的时间同步。

要使用 NTP，请执行以下步骤：

a 在 vSphere Client 中，从清单中选择所需的主机。

b 依次单击**配置**选项卡和**时间配置**。

c 单击面板右上角的**属性**链接。

d 设置时间和日期。

e 选择 **NTP 客户端已启用**以打开 NTP 服务所使用的服务控制台防火墙端口。

3 确保为主机配置的 DNS 服务器可以解析活动目录控制器的主机名。

可以使用 vSphere Client 的“DNS 和路由配置”对话框修改主机的主机名和 DNS 服务器信息。

a 在 vSphere Client 中，从清单中选择所需的主机。

b 依次单击**配置**选项卡和 **DNS 和路由**。

c 单击面板右上角的**属性**链接以访问“DNS 和路由配置”对话框。

下一步

使用 vSphere Client 加入目录服务域。

将主机添加到目录服务域

要使用目录服务，必须将主机加入到目录服务域。

可以使用以下两种方法之一输入域名：

- **name.tld**（例如 **domain.com**）：在默认容器下会创建该帐户。
- **name.tld/container/path**（例如 **domain.com/OU1/OU2**）：在特定组织单元 (OU) 下会创建该帐户。

前提条件

确认 vSphere Client 已连接到 vCenter Server 系统或主机。

步骤

1 在 vSphere Client 清单中选择主机，然后单击**配置**选项卡。

2 在“软件”下，选择**身份验证服务**并单击**属性**。

3 在“目录服务配置”对话框中，从下拉菜单中选择身份验证类型。

选项	描述
如果选择“活动目录”	以 **name.tld** 或 **name.tld/container/path** 形式输入域，然后单击**加入域**。
如果主机已在使用目录服务	选择**离开域**以离开该域并加入另一个域。

4 输入有权将主机加入到域的活动目录用户的用户名和密码，然后单击**确定**。

5 单击**确定**关闭“目录服务配置”对话框。

使用主机配置文件将权限应用到主机

将主机加入活动目录域时，您必须在主机上为该域中的用户或组定义角色。否则，活动目录用户或组将无法访问该主机。可以使用主机配置文件为用户或组设置必需的角色并将更改应用到一个或多个主机。

前提条件

必须已经有主机配置文件。请参见第 196 页，“创建主机配置文件”。

确认要将配置文件应用到的主机处于维护模式。

步骤

1 使用 vSphere Client，选择**视图 > 管理 > 主机配置文件**。

2 右键单击一个现有的主机配置文件，然后选择**编辑配置文件**。

3 展开配置文件树，然后展开**安全配置**。

4 右键单击**权限规则**文件夹，然后选择**添加配置文件**。

5 展开**权限规则**并选择**权限**。

6 在右窗格中的**配置详细信息**选项卡上，单击**配置权限**下拉菜单并选择**需要权限规则**。

7 输入用户和组的名称。

   请使用格式 `DOMAIN\name`，其中 `DOMAIN` 是活动目录域的名称，`name` 是用户名或组名。

8 （可选） 如果输入的名称是组（而非单个用户），请选中**名称指的是用户组**复选框。

9 为用户或组输入已分配的角色名称（通常是 `Admin`）。

   角色名称区分大小写。如果这是一个系统角色，则必须使用未本地化的角色名称。例如，对于管理员角色，请输入 `Admin`。对于只读角色，请输入 `ReadOnly`。

10 选中**传播权限**复选框，并单击**确定**。

下一步

1 将配置文件附加到主机，如第 200 页，“从主机连接实体”中所述。

2 将配置文件应用到主机，如第 200 页，“从主机应用配置文件”中所述。

ESX 加密和安全证书

ESX 支持 SSL v3 和 TLS v1（此处统称为 SSL）。如果启用了 SSL，则数据将是专用的受保护数据，并且只要有人在传输过程中对其进行修改，就将被检测到。

只要以下条件成立，所有网络流量都会进行加密。

- 未对 Web 代理服务作出更改以允许未加密的流量通过端口。
- 服务控制台防火墙的安全性已配置为中和高。

默认情况下启用主机证书检查，并且使用 SSL 证书加密网络流量。但是，ESX 使用安装过程中自动生成的证书，并将此证书存储在主机上。这些证书是唯一的，使用这些证书后便可以开始使用服务器，但它们是不可验证的，而且不是由公认的权威证书授权机构 (CA) 签署的。这些默认证书容易受到中间人攻击的侵害。

若要享受证书检查的最大优势，特别是，如果您要使用加密的外部远程连接，则应安装由有效内部证书授权机构签署的新证书，或从您信任的安全授权机构那里购买新证书。

注意 如果使用的是自签署证书，客户端就会收到关于证书的警告。要解决此问题，请安装由公认的证书颁发机构签署的证书。如果没有安装 CA 签署的证书，则将使用自签署证书加密 vCenter Server 和 vSphere Client 之间的所有通信。这些证书不提供可能在生产环境中需要的身份验证安全性。

证书的默认位置是 ESX 主机上的 `/etc/vmware/ssl/`。证书由两个文件组成：证书本身 (`rui.crt`) 和专用密钥文件 (`rui.key`)。

启用证书检查和验证主机指纹

为防止中间人攻击并充分利用证书提供的安全性，会在默认情况下启用证书检查。可以在 vSphere Client 中验证是否已启用证书检查。

注意 vCenter Server 证书在各次升级中均被保留。

步骤

1 使用 vSphere Client 登录到 vCenter Server 系统。

2 选择**系统管理 > vCenter Server 设置**。

3 在左窗格中单击 **SSL 设置**，然后验证**检查主机证书**是否已选中。

4 如果有需要手动验证的主机，则可以比较主机列出的指纹和主机控制台中的指纹。

要获得 ESX 的主机指纹，请运行以下命令。

```
openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha1 -noout
```

5 如果指纹匹配，则选中主机旁边的**验证**复选框。

单击**确定**之后，未选中的主机将断开连接。

6 单击**确定**。

生成 ESX 主机的新证书

ESX 主机在首次启动系统时生成证书。在某些情况下，可能需要强制主机生成新的证书。通常，只有当更改主机名称或意外删除证书时，才要生成新证书。

在每次重新启动 `vmware-hostd` 进程时，`mgmt-vmware` 脚本都会搜索现有的证书文件（`rui.crt` 和 `rui.key`）。如果未能找到这些文件，则将生成新证书文件。

步骤

1 在 `/etc/vmware/ssl` 目录中，备份现有证书，方法是使用以下命令对其进行重命名。

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

注意 如果由于意外删除了证书而需要重新生成这些证书，则不必对其进行重命名。

2 使用以下命令来重新启动 `vmware-hostd` 进程。

```
service mgmt-vmware restart
```

3 通过执行以下命令并将新证书文件的时间戳与 orig.rui.crt 和 orig.rui.key 进行比较，来确认 ESX 主机已成功生成新证书。

```
ls -la
```

用 CA 签署证书替换默认证书

ESX 主机使用安装过程中自动生成的证书。这些证书是唯一的，使用这些证书后便可以开始使用服务器，但它们是不可验证的，而且不是由公认的权威证书颁发机构 (CA) 签署的。

使用默认证书可能不符合您的组织的安全策略。如果需要可信证书颁发机构颁发的证书，则可以替换默认证书。

注意 如果主机启用了“验证证书”功能，则替换默认证书可能会导致 vCenter Server 停止管理主机。如果新证书不能通过 vCenter Server 验证，则必须使用 vSphere Client 重新连接主机。

步骤

1 登录服务控制台并获取 root 特权。

2 在 `/etc/vmware/ssl` 目录中，使用以下命令重命名现有证书。

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

3 将新证书和密钥复制到 `/etc/vmware/ssl`。

4 将新证书和密钥重命名为 `rui.crt` 和 `rui.key`。

5 重新启动 `vmware-hostd` 进程使证书生效。

```
service mgmt-vmware restart
```

配置 SSL 超时

可以为 ESX 配置 SSL 超时。

可以为两种类型的空闲连接设置超时期间：

- 读取超时设置应用于已完成与 ESX 的端口 443 的 SSL 握手进程的连接。
- 握手超时设置应用于尚未完成与 ESX 的端口 443 的 SSL 握手进程的连接。

这两种连接超时设置均以毫秒为单位。

空闲连接在超过超时时间之后将断开。默认情况下，完全建立的 SSL 连接没有超时限制。

步骤

1 登录服务控制台并获取 root 特权。

2 将目录更改为 `/etc/vmware/hostd/`。

3 使用文本编辑器打开 `config.xml` 文件。

4 输入 `<readTimeoutMs>` 值，以毫秒为单位。

例如，要将读取超时设置为 20 秒，请输入以下命令。

```
<readTimeoutMs>20000</readTimeoutMs>
```

5 输入 `<handshakeTimeoutMs>` 值，以毫秒为单位。

例如，要将握手超时设置为 20 秒，请输入以下命令。

```
<handshakeTimeoutMs>20000</handshakeTimeoutMs>
```

6 保存更改并关闭文件。

7 输入以下命令以重新启动 `vmware-hostd` 进程。

```
service mgmt-vmware restart
```

示例 13–2 配置文件

文件 `/etc/vmware/hostd/config.xml` 的以下部分显示 SSL 超时设置的输入位置。

```
<vmacore>
    ...
<http>
            <readTimeoutMs>20000</readTimeoutMs>
    </http>
    ...
    <ssl>
        ...
        <handshakeTimeoutMs>20000</handshakeTimeoutMs>
        ...
    </ssl>
</vmacore>
```

修改 ESX Web 代理设置

当修改 Web 代理设置时，需要考虑若干加密和用户安全准则。

注意 在更改主机目录或身份验证机制之后，通过输入命令 `service mgmt-vmware restart`，重新启动 `vmware-hostd` 进程。

- 不要使用密码短语设置证书。ESX 不支持密码短语（也称为加密的密钥），如果设置了密码短语，ESX 进程将无法正常启动。
- 您可以配置 Web 代理，以便它在非默认位置中搜索证书。对于倾向于将其证书集中在单台计算机上以便使多台主机可使用证书的公司而言，此功能相当有用。



小心 如果证书不是存储在本地主机上（例如，存储在 NFS 共享主机上），则在 ESX 失去网络连接时主机将无法访问这些证书。因此，连接到主机的客户端无法成功地参与同主机的安全 SSL 握手。

- 为了支持对用户名、密码和数据包进行加密，将在默认情况下针对 vSphere Web Access 和 vSphere Web Services SDK 连接启用 SSL。要配置这些连接以使它们不对传输进行加密，请针对 vSphere Web Access 连接或 vSphere Web Services SDK 连接禁用 SSL，方法是将连接从 HTTPS 切换至 HTTP。

  仅当为这些客户端创建了完全可信的环境时才可考虑禁用 SSL，在这样的环境中，安装有防火墙，而且与主机之间的传输是完全隔离的。禁用 SSL 可提高性能，因为省却了执行加密所需的开销。

- 为了防止误用 ESX 服务（例如，用来托管 vSphere Web Access 的内部 Web 服务器），只能通过用于 HTTPS 传输的端口 443 才能访问大多数内部 ESX 服务。端口 443 用作 ESX 的反向代理。通过 HTTP 欢迎使用页面可看到 ESX 上的服务列表，但如果没有相应的授权，则不能直接访问这些服务。

  可对此配置进行更改，以便可通过 HTTP 连接直接访问各个服务。除非是在完全可信的环境中使用 ESX，否则不要进行此更改。

- 在升级 vCenter Server 和 vSphere Web Access 时，证书保持在原位。如果移除 vCenter Server 和 vSphere Web Access，证书目录不会从服务控制台中移除。

将 Web 代理配置为在非默认位置中搜索证书

您可以配置 Web 代理，以便它在非默认位置中搜索证书。对于将其证书集中在单台计算机上以便使多台主机可使用证书的公司而言，此功能相当有用。

步骤

1 登录服务控制台并获取 root 特权。

2 将目录更改为 `/etc/vmware/hostd/`。

3 使用文本编辑器打开 `proxy.xml` 文件，并找到以下 XML 分段。

```
<ssl>
<!-- The server private key file -->
<privateKey>/etc/vmware/ssl/rui.key</privateKey>
<!-- The server side certificate file -->
<certificate>/etc/vmware/ssl/rui.crt</certificate>
</ssl>
```

4 使用从受信任证书颁发机构接收的专用密钥文件的绝对路径来替换 `/etc/vmware/ssl/rui.key`。

此路径可以位于 ESX 主机上，也可以位于用来存储贵公司的证书和密钥的集中式计算机上。

注意 保持 `<privateKey>` 和 `</privateKey>` XML 标记不变。

5 使用从可信证书颁发机构接收的证书文件的绝对路径来替换 `/etc/vmware/ssl/rui.crt`。



小心 不要删除原始 `rui.key` 和 `rui.crt` 文件。ESX 主机会使用这些文件。

6 保存更改并关闭文件。

7 输入以下命令以重新启动 `vmware-hostd` 进程。

```
service mgmt-vmware restart
```

更改 Web 代理服务的安全设置

可更改此安全配置，以便可通过 HTTP 连接直接访问各种服务。

步骤

1 登录服务控制台并获取 root 特权。

2 将目录更改为 `/etc/vmware/hostd/`。

3 使用文本编辑器打开 `proxy.xml` 文件。

文件内容通常如下所示：

```
<ConfigRoot>
<EndpointList>
<_length>10</_length>
<_type>vim.ProxyService.EndpointSpec[]</_type>
<e id="0">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8309</port>
<serverNamespace>/</serverNamespace>
</e>
<e id="1">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>8309</port>
<serverNamespace>/client/clients.xml</serverNamespace>
</e>
<e id="2">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>12001</port>
<serverNamespace>/ha-nfc</serverNamespace>
</e>
<e id="3">
<_type>vim.ProxyService.NamedPipeServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<pipeName>/var/run/vmware/proxy-mob</pipeName>
<serverNamespace>/mob</serverNamespace>
</e>
<e id="4">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>12000</port>
<serverNamespace>/nfc</serverNamespace>
</e>
<e id="5">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8307</port>
<serverNamespace>/sdk</serverNamespace>
</e>
<e id="6">
<_type>vim.ProxyService.NamedPipeTunnelSpec</_type>
<accessMode>httpOnly</accessMode>
<pipeName>/var/run/vmware/proxy-sdk-tunnel</pipeName>
<serverNamespace>/sdkTunnel</serverNamespace>
</e>
<e id="7">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8308</port>
<serverNamespace>/ui</serverNamespace>
</e>
```

```
<e id="8">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsOnly</accessMode>
<port>8089</port>
<serverNamespace>/vpxa</serverNamespace>
</e>
<e id="9">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8889</port>
<serverNamespace>/wsman</serverNamespace>
</e>
</EndpointList>
</ConfigRoot>
```

4 根据需要更改安全设置。

例如，您可能要修改与使用 HTTPS 的服务相对应的条目，以添加 HTTP 访问选项。

- *e id* 是服务器 ID XML 标记的 ID 编号。ID 编号在 HTTP 区域中必须是唯一的。
- *_type* 是正在移动的服务的名称。
- *accessmode* 是服务允许的通信形式。可接受的值包括：
  - httpOnly - 只能通过纯文本 HTTP 连接来访问服务。
  - httpsOnly - 只能通过 HTTPS 连接来访问服务。
  - httpsWithRedirect - 只能通过 HTTPS 连接来访问服务。通过 HTTP 发出的请求将被重定向到相应的 HTTPS URL。
  - httpAndHttps - 可通过 HTTP 和 HTTPS 两种连接来访问服务。
- *port* 是分配给该服务的端口号。可以为服务分配其他端口号。
- *serverNamespace* 是提供此服务的服务器的命名空间，例如 `/sdk` 或 `/mob`。

5 保存更改并关闭文件。

6 输入以下命令以重新启动 `vmware-hostd` 进程：

```
service mgmt-vmware restart
```

示例 13–3 设置 vSphere Web Access 以通过不安全的端口进行通信

vSphere Web Access 通常通过安全端口 (HTTPS, 443) 与 ESX 主机进行通信。如果处在完全可信的环境中，则可决定几乎可以允许不安全的端口（例如，HTTP, 80）。要执行此操作，请在 `proxy.xml` 文件中更改 Web 服务器的 `accessMode` 属性。在下面的结果中，访问模式将从 `httpsWithRedirect` 更改为 `httpAndHttps`。

```
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>8080</port>
<serverNamespace>/ui</serverNamespace>
```

服务控制台安全 14

VMware 提供使用服务控制台的基本安全建议，包括如何使用服务控制台中内置的一些安全功能。服务控制台是 ESX 的管理界面，因此其安全很关键。为了避免服务控制台遭到未经授权的入侵和误用，VMware 对几个服务控制台参数、设置和活动施加了一些限制。

本章讨论了以下主题：

常规安全建议

为了避免服务控制台遭到未经授权的入侵和误用，VMware 对几个服务控制台参数、设置和活动施加了一些限制。可以根据配置需求而放宽这些限制，但这样做之前，要确保在受信任的环境中工作且已经采取了足够的其他安全措施，以便保护整个网络和连接到 ESX 主机的设备。

评估服务控制台安全和管理服务控制台时请考虑以下建议：

- 限制用户访问。

为了改进安全性，可限制用户访问服务控制台，并实施访问安全策略，如设置密码限制（例如，字符长度、密码时效限制及使用 grub 密码引导主机）。

服务控制台具有访问 ESX 的某些部分的特权。因此，只向信任的用户提供登录访问权限。默认情况下，通过不允许 Secure Shell (SSH) 作为根用户登录来限制根访问权限。强烈建议保持此默认设置。应要求 ESX 系统管理员作为常规用户登录，然后使用 `sudo` 命令来执行需要根特权的特定任务。

另外，请尝试在服务控制台上运行尽可能少的进程。理想情况下，应力争只运行必需的进程、服务和代理，例如病毒检查器、虚拟机备份等等。

- 使用 vSphere Client 管理 ESX 主机。

  尽可能使用 vSphere Client、vSphere Web Access 或第三方网络管理工具来管理 ESX 主机，而不是以 root 用户身份通过命令行界面工作。通过 vSphere Client，可以限制具有服务控制台访问权限的帐户，安全地委派职责，并设置角色以防止管理员和用户使用不必要的功能。

- 仅使用 VMware 源来升级在服务控制台上运行的 ESX 组件。

  服务控制台运行各种第三方软件包（例如 Tomcat Web 服务）来支持管理界面或必须执行的任务。VMware 不支持从 VMware 源以外的任何其他源升级这些软件包。如果使用来自另一个源的下载文件或修补程序，就可能危及服务控制台的安全或功能。定期查看第三方供应商站点和 VMware 知识库，以获知安全警示。

登录到服务控制台

尽管可以通过 vSphere Client 执行大多数 ESX 配置活动，但在配置某些安全功能时也需使用服务控制台命令行界面。使用命令行界面需登录主机。

步骤

1 使用以下方法之一登录 ESX 主机。

   - 如果具有主机的直接访问权限，请在主机的物理控制台上按 Alt+F2 打开登录页面。
   - 如果要远程连接到主机，请使用 SSH 或其他远程控制台连接在主机上启动会话。

2 输入能够由 ESX 主机识别的用户名和密码。

   如果所执行的活动需要 root 特权，请以可识别的用户身份登录服务控制台并通过 `sudo` 命令获取 root 特权，此命令与 `su` 命令相比，提供的安全性更高。

下一步

除了特定于 ESX 的命令外，还可以使用服务控制台命令行界面运行许多 Linux 和 UNIX 命令。有关服务控制台命令的详细信息，可使用 `man` *command_name* 命令查看手册页。

服务控制台防火墙配置

ESX 在服务控制台和网络之间设有防火墙。为了确保服务控制台的完整性，VMware 已经减少了默认情况下打开的防火墙端口数目。

安装时，服务控制台防火墙配置为阻止除端口 22、123、427、443、902、5989 和 5988 之外的所有输入和输出流量，这些端口用于与 ESX 进行基本通信。此设置强制了主机的高安全级别。

注意 此防火墙还允许 Internet 控制消息协议 (ICMP) ping 及与 DHCP 和 DNS（仅 UDP）客户端的通信。

在受信任的环境中，您可能认为可以接受较低的安全级别。此时，可将防火墙设置为中等安全或低安全级别。

中等安全级别 除了默认端口以及明确打开的任何端口外，阻止其他所有输入流量。不阻止输出流量。

低安全级别 不阻止输入流量和输出流量。该设置等同于移除防火墙。

由于默认情况下打开的端口受到严格的限制，因此安装之后可能需要打开其他端口。有关可能要打开的常用端口列表，请参见第 143 页，“用于管理访问的 TCP 和 UDP 端口”。

当添加有效操作 ESX 所需的支持服务和管理代理时，需要打开服务控制台防火墙中的其他端口。您可以通过 vCenter Server 添加服务和管理代理，如第 141 页，“为支持的服务和管理代理配置防火墙端口”中所述。

除了为这些服务和代理打开的端口之外，当配置某些设备、服务或代理（如存储设备、备份代理和管理代理等）时也可能需要打开其他端口。例如，如果将 Veritas NetBackup™ 4.5 用作备份代理，则需要打开端口 13720、13724、13782 和 13783，NetBackup 将这些端口用于客户端介质事务、数据库备份、用户备份或恢复等。要确定打开哪些端口，请参见设备、服务或代理的供应商规范。

注意 不要使用 `esxcfg-firewall` 以外的任何命令或实用程序来修改服务控制台的默认防火墙规则。如果使用 Linux 命令修改默认值，所做的更改将会被忽略，并由 `esxcfg-firewall` 命令为该服务指定的默认值覆盖。

确定服务控制台防火墙安全级别

更改服务控制台的安全级别的过程分为两步：确定服务控制台防火墙安全级别和重置服务控制台防火墙设置。为了避免不必要的步骤，请始终在更改防火墙设置之前对其进行检查。

步骤

1 登录服务控制台并获取 root 特权。

2 使用以下两条命令确定是阻止还是允许入站和出站流量。

```
esxcfg-firewall -q incoming
esxcfg-firewall -q outgoing
```

根据表 14–1 解释结果。

表 14–1 服务控制台防火墙安全级别

命令行响应	安全级别
默认情况下阻止入站端口。 默认情况下阻止出站端口。	高
默认情况下阻止入站端口。 默认情况下不阻止出站端口。	中等
默认情况下不阻止入站端口。 默认情况下不阻止出站端口。	低

设置服务控制台防火墙安全级别

确定服务控制台的防火墙安全级别后，可以设置安全级别。每次降低安全设置或打开其他端口时，都会提高网络中的入侵风险。应在访问需求和网络安全控制程度之间寻求平衡。

步骤

1 登录服务控制台并获取 root 特权。

2 运行以下命令之一，设置服务控制台防火墙安全级别。

- 将服务控制台防火墙设置为中等安全级别：

```
esxcfg-firewall --allowOutgoing --blockIncoming
```

- 将虚拟防火墙设置为低安全级别：

```
esxcfg-firewall --allowIncoming --allowOutgoing
```



小心 使用上述命令将禁用所有防火墙保护。

- 将服务控制台防火墙恢复为高安全级别：

```
esxcfg-firewall --blockIncoming --blockOutgoing
```

3 使用以下命令来重新启动 `vmware-hostd` 进程。

```
service mgmt-vmware restart
```

更改服务控制台防火墙安全级别不会影响现有连接。例如，如果防火墙设置为低安全级别且正在未明确打开的端口上运行备份，则将防火墙设置提升为高安全级别不会终止此备份。备份随即完成，系统会释放连接，而且端口将不接受进一步的连接。

在服务控制台防火墙中打开端口

安装第三方设备、服务和代理时，可以打开服务控制台防火墙端口。打开端口以支持正在安装的项目之前，请参见供应商规范以确定必需的端口。

前提条件

此过程仅用于打开不能通过 vSphere Client 配置的服务或代理的端口。



小心 VMware 仅支持通过 vSphere Client 或 `esxcfg-firewall` 命令打开和关闭防火墙端口。使用任何其他方法或脚本打开防火墙端口可能会导致意外行为。

步骤

1 登录服务控制台并获取 root 特权。

2 使用以下命令打开端口。

```
esxcfg-firewall --openPort port_number,tcp|udp,in|out,port_name
```

- *port_number* 是供应商指定的端口号。
- 对于 TCP 流量使用 `tcp`，或者对于 UDP 流量使用 `udp`。
- 使用 `in` 为输入流量打开端口，或者使用 `out` 为输出流量打开端口。
- *port_name* 是一个描述性名称，有助于标识使用该端口的服务或代理。唯一名称不是必需的。

例如：

```
esxcfg-firewall --openPort 6380,tcp,in,Navisphere
```

3 通过运行以下命令来重新启动 `vmware-hostd` 进程。

```
service mgmt-vmware restart
```

在服务控制台防火墙中关闭端口

可以在服务控制台防火墙中关闭特定端口。在关闭某个端口时，不一定会断开与该端口关联的服务的活动会话。例如，如果您在执行备份时关闭备份代理的端口，则备份将继续，直到备份完成及代理释放连接。

使用 `-closePort` 选项只能关闭借助于 `-openPort` 选项打开的端口。如果端口是用其他方法打开的，则需要使用等效方法来关闭该端口。例如，只能通过在 vSphere Client 中禁用 SSH 服务器入站连接和 SSH 客户端出站连接来关闭 SSH 端口 (22)。

前提条件

此过程仅用于关闭不能通过 vSphere Client 进行明确配置的服务或代理的端口。



小心 VMware 仅支持通过 vSphere Client 或 `esxcfg-firewall` 命令打开和关闭防火墙端口。使用任何其他方法或脚本打开和关闭防火墙端口可能会导致意外行为。

步骤

1 登录服务控制台并获取 root 特权。

2 使用以下命令关闭端口。

```
esxcfg-firewall --closePort port_number,tcp|udp,in|out,port_name
```

port_name 为可选参数。

例如：

```
esxcfg-firewall --closePort 6380,tcp,in
```

3 使用以下命令来重新启动 `vmware-hostd` 进程。

```
service mgmt-vmware restart
```

防火墙被覆盖时的故障排除

在 VMware High Availability (HA) 通信、迁移、克隆、修补或 vMotion 之后更改防火墙规则时，可能需要配置 esxcfg-firewall 的默认值。

不支持使用 esxcfg-firewall 以外的任何命令或实用程序来修改服务控制台的默认防火墙规则。如果使用任何工具或实用程序修改默认规则，然后尝试通过防火墙访问服务控制台，则在操作完成后防火墙可能会恢复为其默认配置。例如，如果已使用 esxcfg-firewall 之外的命令修改了规则，则在主机上配置 HA 会导致防火墙恢复为由 esxcfg-firewall 指定的默认配置。

在大多数情况下，您无需更改服务控制台的默认防火墙规则。如果使用 Linux 命令修改默认值，所做的更改将会被忽略，并由 esxcfg-firewall 命令为该服务指定的默认值覆盖。如果要更改所支持服务的默认值，或定义其他服务类型的默认值，可以在 /etc/vmware/firewall/chains/default.xml 中修改或添加规则。

步骤

1 使用管理员特权登录服务控制台。
2 编辑 /etc/vmware/firewall/chains/default.xml 文件使之与安全策略对应。
3 使用 service firewall restart 命令重新启动服务控制台防火墙。
4 使用 esxcfg-firewall-e|d SERVICE 命令检查指定的服务是否已正确启用或禁用。

示例 14–1 修改 INPUT 链

可以根据自己的安全策略来修改每种服务类型的防火墙默认值。例如，/etc/vmware/firewall/chains/default.xml 文件中的以下规则将确定 INPUT 链的防火墙规则：

```
<ConfigRoot>
<chain name="INPUT">
<rule>-p tcp --dport 80 -j ACCEPT</rule>
<rule>-p tcp --dport 110 -j ACCEPT</rule>
<rule>-p tcp --dport 25 -j ACCEPT</rule>
</chain>...
</ConfigRoot>
```

密码限制

攻击者登录 ESX 主机的难易程度取决于是否可找到合法用户名/密码组合。可以设置密码限制来帮助阻止攻击者获得用户密码。

恶意用户可以通过许多方式获得密码。例如，攻击者可以嗅探不安全的网络流量（例如 Telnet 或 FTP 传输）来尝试成功登录。另一种破解密码的常见方法是：通过运行密码生成器，尝试达到某一长度的每种字符组合或者使用实际单词和实际单词的简单变种。

实施用来管理密码长度、字符集和持续时间的限制可让密码生成器启动的攻击变得更加困难。密码越长越复杂，攻击者就越难发现密码。用户更改密码越频繁，就越难找到反复奏效的密码。

注意 在决定如何实施密码限制时，要始终考虑到人因素。如果这些限制使得密码难以记住或强制进行频繁的密码更改，用户可能倾向于写下自己的密码，导致事与愿违。

为了避免密码数据库遭到误用，启用了密码遮蔽，以便隐藏密码哈希值，使其无法访问。此外，ESX 使用 MD5 密码哈希值提供更强的密码安全，并让您将最小长度要求设置为八个字符以上。

密码时效

可以施加密码时效限制，以确保用户密码不会长期保持活动状态。

默认情况下，ESX 对用户登录施加以下密码时效限制。

最大天数 用户可以保持密码的天数。默认情况下，密码永不过期。

最小天数 两次密码更改之间相隔的最小天数。默认为 0 天，这意味着用户可以随时更改其密码。

警告时间 在密码到期之前需要提前发送提醒的天数。默认值为七天。只有直接登录服务控制台或使用 SSH 时才会显示警告。

可以加强或放松以上任何设置。还可以覆盖单个用户或组的默认密码时效设置。

更改主机的默认密码时效限制

可以为主机施加比默认提供的更为严格或宽松的密码时效限制。

步骤

1 登录服务控制台并获取 root 特权。

2 要更改用户可保留密码的最大天数，请使用以下命令。

```
esxcfg-auth --passmaxdays=number_of_days
```

3 要对两次密码更改之间相隔的最小天数进行更改，请使用以下命令。

```
esxcfg-auth --passmindays=number_of_days
```

4 要更改密码更改之前的警告时间，请使用以下命令。

```
esxcfg-auth --passwarnage=number_of_days
```

更改用户的默认密码时效限制

可以覆盖特定用户或组的默认密码时效限制。

步骤

1 登录服务控制台并获取 root 特权。

2 要更改最大天数，请使用以下命令。

```
chage -M number_of_days username
```

3 要更改警告时间，请使用以下命令。

```
chage -W number_of_days username
```

4 要更改最小天数，请使用以下命令。

```
chage -m number_of_days username
```

密码强度和复杂度

默认情况下，ESX 使用 `pam_passwdqc.so` 插件来设置用户创建密码时必须遵守的规则并检查密码强度。

通过 `pam_passwdqc.so` 插件，可以确定所有密码必须达到的基本标准。默认情况下，ESX 不对根密码施加任何限制。然而，当非 root 用户尝试更改密码时，所选择的密码必须符合 `pam_passwdqc.so` 设定的基本标准。

有效密码应该包含尽可能多的字符种类的组合。字符种类包括小写字母、大写字母、数字和特殊字符（如下划线或短划线）。

注意 在计算字符种类的数目时，该插件不会将密码的第一个大写字母以及密码的最后一个数字字符计算在内。

要配置密码复杂性，可以更改下列参数的默认值。

- *N0* 是仅使用一种字符时密码所需的字符数。例如，密码只包含小写字母。
- *N1* 是使用两种字符时密码所需的字符数。
- *N2* 用于密码短语。ESX 要求密码短语由三个单词组成。密码短语中每个单词的长度都必须介于 8-40 个字符之间。
- *N3* 是使用三种字符时密码所需的字符数。
- *N4* 是使用全部四种字符时密码所需的字符数。
- *match* 是从旧密码重用的字符串中所允许的字符数。如果 `pam_passwdqc.so` 插件找到此长度或更长的重用字符串，将认定此字符串无法通过强度测试并仅使用剩余的字符。

将上述任何选项设置为 `-1` 可指示 `pam_passwdqc.so` 插件忽略此要求。

将上述任何选项设置为 `disabled` 可指示 `pam_passwdqc.so` 插件认定具有关联特性的密码不符合要求。除 `-1` 和 `disabled` 之外，所用的值必须采用递减顺序。

注意 用于 Linux 的 `pam_passwdqc.so` 插件提供的参数多于 ESX 支持的参数。您不能在 `esxcfg-auth` 中指定这些其他参数。

有关 `pam_passwdqc.so` 插件的详细信息，请参见 Linux 文档。

更改 pam_passwdqc.so 插件的默认密码复杂性

配置 `pam_passwdqc.so` 插件以确定所有密码必须满足的基本标准。

步骤

1 登录服务控制台并获取 root 特权。

2 输入以下命令。

```
esxcfg-auth --usepamqc=N0N1N2N3N4match
```

示例 14–2 esxcfg-auth --usepamqc 命令

例如，您使用以下命令。

```
esxcfg-auth --usepamqc=disabled 18 -1 12 8
```

如果实行此设置，用户创建密码时将无法设置仅包含一种字符的密码。用户需要对两种字符组成的密码至少使用 18 个字符，对三种字符组成的密码至少使用 12 个字符，对四种字符组成的密码至少使用 8 个字符。创建密码短语的尝试将被忽略。

配置密码重用规则

可以设置为每位用户存储的旧密码数目。

步骤

1 登录服务控制台并获取 root 特权。

2 将目录更改到 `/etc/pam.d/`。

3 使用文本编辑器打开 `system-auth-generic` 文件。

4 查找以 password sufficient /lib/security/$ISA/pam_unix.so 开头的行。

5 将以下参数添加到该行的末尾，其中，X 是为每位用户存储的旧密码数。

```
remember=X
```

在参数之间使用空格。

6 保存更改并关闭文件。

7 将目录更改为 /etc/security/，并使用以下命令生成文件名为 opasswd 的零 (0) 长度文件。

```
touch opasswd
```

8 输入下列命令：

```
chmod 0600 opasswd
chown root:root /etc/security/opasswd
```

使用 pam_cracklib.so 身份验证插件

ESX 的默认身份验证插件为 pam_passwdqc.so，它可为大多数环境提供严格执行的密码强度。如果该插件不适合您的环境，可以改用 pam_cracklib.so 插件。

pam_cracklib.so 插件会检查所有密码更改尝试以确保密码满足强度标准。

- 新密码不得是回文。回文是指其中心字母两边的字母完全相同的词，如 radar 或 civic。
- 新密码不得是旧密码的逆序。
- 新密码不得通过旋转形成。旋转形成的新密码是旧密码的一种变体，将旧密码的一个或多个字符旋转到密码字符串的前面或后面。
- 新密码与旧密码的差异不能只是更改了大小写。
- 新密码与旧密码的区别不能只是几个字符不同。
- 新密码不得在过去已经用过。只有在配置了密码重用规则的情况下，pam_cracklib.so 插件才会应用此标准。

  默认情况下，ESX 不强制实施任何密码重用规则，因此 pam_cracklib.so 插件决不会以这些理由拒绝密码更改尝试。但是，您可以配置重用规则以确保用户不是轮流使用几个密码。

  如果配置重用规则，旧密码会存储到 pam_cracklib.so 插件在每次密码更改尝试期间引用的文件内。重用规则将确定 ESX 保留的旧密码数目。当用户创建的密码达到了重用规则指定的值时，旧密码将按照新旧顺序从文件中移除。
- 新密码必须具有足够的长度和复杂度才能满足插件的要求。通过使用 esxcfg-auth 命令更改 pam_cracklib.so 复杂度参数可配置这些要求，此命令可让您设置重试次数、最小密码长度和各种字符信用。

要使用 pam_cracklib.so 插件设置密码复杂性，可以为下列每个字符种类的信用参数指定值：

- *lc_credit* 表示小写字母
- *uc_credit* 表示大写字母
- *d_credit* 表示数字
- *oc_credit* 表示特殊字符（如下划线或短划线）

信用会增加密码的复杂度评分。用户的密码必须达到或超过最低评分，最低评分是通过使用 *minimum_length* 参数定义的。

注意 无论使用的信用如何，也无论分配给 *minimum_length* 的值为多大，pam_cracklib.so 插件不接受少于 6 个字符的密码。换言之，如果 *minimum_length* 为 5，用户仍必须输入不少于 6 个字符。

为确定密码是否可接受，pam_cracklib.so 插件使用多个规则来计算密码评分。

- 对于 *minimum_length*，密码中的每个字符（无论是何种类型）都算一个字符。
- 根据所使用的是负值还是正值，信用参数中的非零值对密码复杂度的影响会不同。
  - 对于正值，将为这种字符增加一个信用，最多增加由信用参数指定的最大数目的信用。

    例如，如果 *lc_credit* 为 1，将为在密码中使用小写字母增加一个信用。这种情况下，1 是使用小写字母所允许的最大数目的信用，无论使用了多少小写字母。
  - 对于负值，不会为这种字符增加信用，但要求这种字符的使用次数至少达到最少次数。该最少次数是由信用参数指定的。

    例如，如果 *uc_credit* 为 -1，则密码至少必须包含一个大写字符。这种情况下，不会为使用大写字母提供额外的信用，无论使用了多少大写字母。
- 如果某几种字符的值为零，则这些字符会计入密码的总长度，但不会获得额外的信用，也不会要求使用次数。可以将所有种类的字符设置为零，以执行密码长度而不考虑复杂度。

  例如，密码 **xyzpqets** 和 **Xyzpq3#s** 的密码评分都是 8。

切换到 pam_cracklib.so 插件

与 pam_passwdqc.so 相比，pam_cracklib.so 插件提供的用于精确调整密码强度的选项更少，并且不针对所有用户执行密码强度测试。但是，如果 pam_cracklib.so 插件更适合您的环境，则可以从默认 pam_passwdqc.so 插件切换为 pam_cracklib.so。

注意 用于 Linux 的 pam_cracklib.so 插件提供的参数多于 ESX 支持的参数。您不能在 esxcfg-auth 中指定这些其他参数。有关该插件的详细信息，请参见 Linux 文档。

步骤

1 登录服务控制台并获取 root 特权。

2 运行下列命令。

```
esxcfg-auth --usecrack=retriesminimum_lengthlc_credituc_creditd_creditoc_credit
```

- *retries*：在锁定之前允许用户重试的次数。
- *minimum_length*:应用信用后的密码最低评分或有效长度。

  注意 无论使用的信用如何，也无论分配给 *minimum_length* 的值为多大，pam_cracklib.so 插件不接受少于 6 个字符的密码。换言之，如果 *minimum_length* 为 5，用户仍必须输入不少于 6 个字符。

- *lc_credit*:小写字母允许的最大信用数。
- *uc_credit*:大写字母允许的最大信用数。
- *d_credit*:数字允许的最大信用数。
- *oc_credit*:特殊字符（如下划线或短划线）允许的最大信用数。

插件的密码要求是根据所输入的参数配置的。

示例 14–3 esxcfg-auth --usecrack 命令

```
esxcfg-auth --usecrack=3 9 1 -1 -1 1
```

- 用户尝试输入三次密码之后，即会被锁定。
- 密码评分必须为 9。
- 使用小写字母最多获得一个信用。
- 要求至少包含一个大写字母。这种字符类型不会获得任何额外的信用。
- 要求至少包含一个数字。这种字符类型不会获得任何额外的信用。
- 使用特殊字符最多获得一个信用。

使用这些示例值，候选密码 **xyzpqe#** 会失败：

```
(x + y + z + p +q + e + #) + (lc_credit + oc_credit) = 9
```

虽然密码评分为 9，但它不包含必需的大写字母和数字。

会接受候选密码 **Xyzpq3#**：

```
(X + y + z + p +q + 3 + #) + (lc_credit + oc_credit) = 9
```

此示例的密码评分也是 9，但此密码包含必需的大写字母和数字。大写字母和数字不增加额外信用。

密码强度

通过不安全的连接传输数据会带来安全风险，因为数据通过网络传输时，恶意用户可能会扫描到这些数据。作为一项安全措施，网络组件通常对数据加密，以防止他人轻松读取这些数据。

为了加密数据，发送组件（如网关或重定向程序）会应用算法或密码，在传输数据之前改变这些数据。接收组件使用密钥解密这些数据，将其还原为原始形式。目前有几种密码正在使用，每种密码提供的安全级别也有所差异。密码保护数据的能力的一种衡量方法是其密码强度，即加密密钥的位数。位数越大，密码越安全。

为了确保对外部网络连接之间的数据传输进行保护，ESX 采用了目前可用的最强大的块密码之一，即 256 位 AES 块加密。ESX 还将 1024 位 RSA 用于密钥交换。这些加密算法是下列连接的默认算法。

- vSphere Client 通过服务控制台与 vCenter Server 和 ESX 主机的连接。
- vSphere Web Access 通过服务控制台与 ESX 主机的连接。

  注意 由于 vSphere Web Access 密码使用情况由所使用的 Web 浏览器确定，因此该管理工具可能使用其他密码。

- SDK 与 vCenter Server 和 ESX 的连接。
- 服务控制台通过 VMkernel 与虚拟机的连接。
- SSH 通过服务控制台与 ESX 主机的连接。

setuid 和 setgid 标记

ESX 安装期间，默认情况下将安装若干个包括 `setuid` 和 `setgid` 标记的应用程序。其中一些应用程序提供了正确运行主机所需的功能。另一些则是可选的，但是它们可以简化主机和网络的维护和故障排除。

setuid
一种标记，通过将有效用户 ID 设置为程序所有者的用户 ID，允许应用程序临时更改运行该应用程序的用户权限。

setgid
一种标记，通过将有效组 ID 设置为程序所有者的组 ID，允许应用程序临时更改运行该应用程序的组权限。

禁用可选应用程序

禁用任何必需的应用程序都将使 ESX 身份验证和虚拟机运行出现问题，但您可以禁用任何可选应用程序。

可选应用程序在表 14-2 和表 14-3 中列出。

步骤

1 登录服务控制台并获取 root 特权。

2 运行以下命令之一，以禁用应用程序。

- 对于附有 `setuid` 标记的应用程序：

  `chmod a-s` *`path_to_executable_file`*

- 对于附有 `setgid` 标记的应用程序：

  `chmod a-g` *`path_to_executable_file`*

默认 setuid 应用程序

默认情况下将安装若干个包括 `setuid` 标记的应用程序。

表 14-2 列出了默认的 `setuid` 应用程序，并指示应用程序是必需的还是可选的。

表 14-2 默认 setuid 应用程序

应用程序	用途和路径	必需或可选
`crontab`	允许个别用户添加 cron 作业。 路径：`/usr/bin/crontab`	可选
`pam_timestamp_check`	支持密码身份验证。 路径：`/sbin/pam_timestamp_check`	必需
`passwd`	支持密码身份验证。 路径：`/usr/bin/passwd`	必需
`ping`	发送和侦听网络接口上的控制数据包。可用于调试网络。 路径：`/bin/ping`	可选
`pwdb_chkpwd`	支持密码身份验证。 路径：`/sbin/pwdb_chkpwd`	必需
`ssh-keysign`	对 SSH 执行基于主机的身份验证。 路径：`/usr/libexec/openssh/ssh-keysign`	如果使用基于主机的身份验证，则为必需。否则为可选。
`su`	通过更改用户，可以使普通用户成为 root 用户。 路径：`/bin/su`	必需
`sudo`	仅针对特定操作让普通用户充当 root 用户。 路径：`/usr/bin/sudo`	可选
`unix_chkpwd`	支持密码身份验证。 路径：`/sbin/unix_chkpwd`	必需
`vmkload_app`	执行运行虚拟机所需的任务。该应用程序安装在两个位置中：一个用于标准用途，一个用于调试。 标准用途的路径：`/usr/lib/vmware/bin/vmkload_app` 调试的路径：`/usr/lib/vmware/bin-debug/vmkload_app`	两个路径均为必需

表 14–2 默认 setuid 应用程序（续）

应用程序	用途和路径	必需或可选
vmware-authd	对使用 VMware 特定服务的用户进行身份验证。 路径：/usr/sbin/vmware-authd	必需
vmware-vmx	执行运行虚拟机所需的任务。该应用程序安装在两个位置中：一个用于标准用途，一个用于调试。 标准用途的路径：/usr/lib/vmware/bin/vmware-vmx 调试的路径：/usr/lib/vmware/bin-debug/vmware-vmk	两个路径均为必需

默认 setgid 应用程序

默认情况下将安装两个包括 setgid 标记的应用程序。

表 14-3 列出了默认的 setgid 应用程序，并指明应用程序是必需的还是可选的。

表 14–3 默认 setgid 应用程序

应用程序	用途和路径	必需或可选
wall	提醒所有终端某个操作即将发生。该应用程序由 shutdown 和其他命令调用。 路径：/usr/bin/wall	可选
lockfile	对于 Dell OM 管理代理执行锁定。 路径：/usr/bin/lockfile	对于 Dell OM 是必需的，否则是可选的

SSH 安全

SSH 是常用的 Unix 和 Linux Command Shell，可以用于远程登录服务控制台并为主机执行某些管理和配置任务。SSH 用于安全登录和数据传输，因为它可提供比其他 Command Shell 更强大的保护。

在此 ESX 版本中，SSH 配置得到了增强，能够提供更高的安全级别。此次功能增强包括以下主要功能。

- 禁用第 1 版 SSH 协议 – VMware 不再支持第 1 版 SSH 协议，而是以独占方式使用第 2 版协议。第 2 版消除了第 1 版中存在的某些安全问题，且提供了更安全的与服务控制台相连的通信接口。
- 提高了加密强度 – SSH 目前对连接仅支持 256 位和 128 位 AES 密码。
- 限制以 root 用户身份进行远程登录 – 不能再以 root 用户身份远程登录。而是以可识别的用户身份登录，并使用 sudo 命令运行需要 root 特权的特定操作，或输入 su 命令成为 root 用户。

注意 sudo 命令具有安全优势，因为它可限制根活动，并通过对用户执行的任何根活动生成审核记录来帮助您检查可能存在的 root 特权误用情况。

这些设置旨在为通过 SSH 传输到服务控制台的数据提供可靠保护。如果此配置对您的需求而言过于严格，可以降低安全参数。

更改默认 SSH 配置

可以更改默认 SSH 配置。

步骤

1 登录服务控制台并获取 root 特权。

2 更改到 /etc/ssh 目录。

3 使用文本编辑器在 `sshd_config` 文件中执行以下任意操作。

- 要允许远程根登录，可在下行中将设置更改为 `yes`。

  ```
  PermitRootLogin no
  ```

- 要恢复为默认 SSH 协议（第 1 版和第 2 版），可注释掉下行。

  ```
  Protocol 2
  ```

- 要恢复为 3DES 密码或其他密码，可注释掉下行。

  ```
  Ciphers aes256-cbc,aes128-cbc
  ```

- 要禁用 SSH 上的安全 FTP (SFTP)，可注释掉下行。

  ```
  Subsystem ftp /usr/libexec/openssh/sftp-server
  ```

4 保存更改并关闭文件。

5 通过运行以下命令来重新启动 SSHD 服务。

```
service sshd restart
```

安全修补程序和安全漏洞扫描软件

某些安全扫描程序（如 Nessus）在搜索安全漏洞时会检查版本号，但不检查修补程序后缀。因此，这些扫描程序可能误报软件安全级别为低且没有包括最新的安全修补程序（即使已经包括）。如果出现此情况，可以执行某些检查。

此问题在业界较常见，不是 VMware 特有的。一些安全扫描程序能够正确处理这种情形，但通常滞后一个版本或多个版本。例如，Red Hat 修补程序之后发布的 Nessus 版本通常不会报告这些错误情况。

如果 VMware 将某个支持 Linux 的软件包作为服务控制台组件（例如服务、功能或协议）提供，而目前该软件包的修补程序可用，VMware 将提供包含“vSphere 安装捆绑包 (VIB)”列表的公告，用于在 ESX 上更新该软件。尽管可以从其他源获得这些修补程序，但请始终使用 VMware 生成的公告，而不是使用第三方“RPM 软件包管理器”包。

当向软件包提供修补程序时，VMware 的策略是将此修补程序反向移植到已知稳定的软件版本中。这种方法减少了在软件中引发新问题和不稳定性的几率。因为修补程序是添加到现有版本的软件中，因此软件的版本号保持不变，但会添加修补程序编号作为后缀。

下面举例说明了此问题是如何出现的：

1 您最初安装了含 OpenSSL 0.9.7a 版本（其中 0.9.7a 是不含修补程序的原始版本）的 ESX。

2 OpenSSL 发布了用来修复 0.9.7 版本中安全漏洞的修补程序。此版本称为 0.9.7x。

3 VMware 将 OpenSSL 0.9.7x 修补程序反向移植到原始版本，更新修补程序编号，并创建 VIB。VIB 中的 OpenSSL 版本为 0.9.7a-1，表示原始版本 (0.9.7a) 现在包含第 1 个修补程序。

4 安装更新。

5 安全扫描程序未能注意到 -1 后缀，误报 OpenSSL 的安全级别不是最新的。

如果扫描程序报告软件包的安全级别较低，请执行以下检查。

- 查看修补程序后缀以确定是否需要进行更新。
- 阅读 VMware VIB 文档，了解有关修补程序内容的信息。
- 从软件更新更改日志的安全警示中查找通用漏洞披露 (CVE) 号。

  如果存在此 CVE 号，则指定的软件包将修补该漏洞。

安全性最佳做法与方案 15

一系列 ESX 部署方案可帮助您了解如何以最佳方式在自己的部署中使用安全功能。方案还提出了若干基本的安全建议，供您在创建和配置虚拟机时参考。

本章讨论了以下主题：

- 第 185 页，“常见 ESX 部署的安全措施”
- 第 188 页，“虚拟机建议”

常见 ESX 部署的安全措施

可以对不同类型的部署的安全措施进行比较，以帮助制定 ESX 部署的安全计划。

根据公司规模、数据及资源与外界共享的方式、有多个数据中心还是只有一个数据中心等因素，ESX 部署的复杂度会有极大差异。以下部署的实质在于用户访问、资源共享及安全级别的策略。

单客户部署

在单客户部署中，ESX 主机由单个公司所有，并在单个数据中心内进行维护。主机资源不与外部用户共享。主机上运行多台虚拟机，并由一名站点管理员进行维护。

此类单客户部署不允许存在客户管理员，维护众多虚拟机的工作由站点管理员独自负责。公司配备一组不具有主机帐户的系统管理员，他们无法访问 vCenter Server 或主机 Command Line Shell 等任何 ESX 工具。这些系统管理员可以通过虚拟机控制台访问虚拟机，因此可以在虚拟机内部加载软件和执行其他维护任务。

表 15‑1 显示了配置用于主机的组件共享的处理方式。

表 15‑1 单客户部署中的组件共享

功能	配置	备注
服务控制台与虚拟机是否共享同一个物理网络?	否	通过为服务控制台配置专用物理网络来对其进行隔离。
服务控制台是否与虚拟机共享同一个 VLAN?	否	通过为服务控制台配置专用 VLAN 来对其进行隔离。虚拟机或其他系统设施（如 vMotion）不一定非要使用此 VLAN。
多个虚拟机是否共享同一个物理网络?	是	将这些虚拟机配置在同一个物理网络中。
是否共享网络适配器?	局部	通过为服务控制台配置专用虚拟交换机和虚拟网络适配器来对其进行隔离。虚拟机或其他系统设施不一定非要使用此交换机或适配器。 可以在同一个虚拟交换机和网络适配器上配置虚拟机。
是否共享 VMFS?	是	所有 `.vmdk` 文件均驻留在同一个 VMFS 分区中。

表 15–1 单客户部署中的组件共享 （续）

功能	配置	备注
安全级别	高	逐个打开 FTP 等所需服务的端口。有关安全级别的信息，请参见第 172 页，“服务控制台防火墙配置”。
虚拟机内存是否过量使用?	是	为虚拟机配置的总内存多于总物理内存。

表 15–2 显示了设置主机用户帐户的方式。

表 15–2 单客户部署中的用户帐户设置

用户类别	帐户总数
站点管理员	1
客户管理员	0
系统管理员	0
商业用户	0

表 15–3 显示了每个用户的访问级别。

表 15–3 单客户部署中的用户访问

访问级别	站点管理员	系统管理员
是否具有根用户访问权限?	是	否
是否通过 SSH 进行服务控制台访问?	是	否
vCenter Server 和 vSphere Web Access?	是	否
是否创建和修改虚拟机?	是	否
是否通过控制台进行虚拟机访问?	是	是

多客户限制部署

在多客户限制部署中，ESX 主机位于同一个数据中心内，并用于为多名客户提供应用程序。这些主机由一名站点管理员维护，并运行多台客户专用的虚拟机。属于不同客户的虚拟机可以位于同一台主机上，但站点管理员会限制资源共享，以避免欺诈性交互。

虽然只有一名站点管理员，但有多名客户管理员维护分配给其客户的虚拟机。此类部署还包括一些客户系统管理员，他们没有 ESX 帐户，但可以通过虚拟机控制台访问虚拟机以加载软件并执行虚拟机内部的其他维护任务。

表 15–4 显示了配置用于主机的组件共享的处理方式。

表 15–4 多客户限制部署中的组件共享

功能	配置	备注
服务控制台与虚拟机是否共享同一个物理网络?	否	通过为服务控制台配置专用物理网络来对其进行隔离。
服务控制台是否与虚拟机共享同一个 VLAN?	否	通过为服务控制台配置专用 VLAN 来对其进行隔离。虚拟机或其他系统设施（如 vMotion）不一定非要使用此 VLAN。
多个虚拟机是否共享同一个物理网络?	局部	将每位客户的虚拟机放置到不同的物理网络中。所有物理网络均相互独立。
是否共享网络适配器?	局部	通过为服务控制台配置专用虚拟交换机和虚拟网络适配器来对其进行隔离。虚拟机或其他系统设施不一定非要使用此交换机或适配器。 将一位客户的多个虚拟机配置为可共享同一台虚拟交换机和同一块网络适配器。它们不与任何其他客户共享交换机和适配器。

表 15–4 多客户限制部署中的组件共享 （续）

功能	配置	备注
是否共享 VMFS?	否	每位客户都有自己的 VMFS 分区，而且虚拟机的 .vmdk 文件以独占方式驻留于该分区。该分区可跨多个 LUN。
安全级别	高	根据需要打开 FTP 等服务的端口。
虚拟机内存是否过量使用?	是	为虚拟机配置的总内存多于总物理内存。

表 15–5 显示了设置 ESX 主机用户帐户的方式。

表 15–5 多客户限制部署中的用户帐户设置

用户类别	帐户总数
站点管理员	1
客户管理员	10
系统管理员	0
商业用户	0

表 15–6 显示了每个用户的访问级别。

表 15–6 多客户限制部署中的用户访问

访问级别	站点管理员	客户管理员	系统管理员
是否具有根用户访问权限?	是	否	否
是否通过 SSH 进行服务控制台访问?	是	是	否
vCenter Server 和 vSphere Web Access?	是	是	否
是否创建和修改虚拟机?	是	是	否
是否通过控制台进行虚拟机访问?	是	是	是

多客户开放部署

在多客户开放部署中，ESX 主机位于同一个数据中心内，并用于为多名客户提供应用程序。这些主机由一名站点管理员维护，并运行多台客户专用的虚拟机。属于不同客户的虚拟机可以位于同一台主机上，但资源共享限制可能更少。

多客户开放部署中虽然只有一名站点管理员，但有多名客户管理员维护分配给其客户的虚拟机。此类部署还包括一些客户系统管理员，他们没有 ESX 帐户，但可以通过虚拟机控制台访问虚拟机以加载软件并执行虚拟机内部的其他维护任务。最后，一组没有帐户的商业用户可以使用虚拟机运行其应用程序。

表 15–7 显示了配置用于主机的组件共享的处理方式。

表 15–7 多客户开放部署中的组件共享

功能	配置	备注
服务控制台与虚拟机是否共享同一个物理网络?	否	通过为服务控制台配置专用物理网络来对其进行隔离。
服务控制台是否与虚拟机共享同一个 VLAN?	否	通过为服务控制台配置专用 VLAN 来对其进行隔离。虚拟机或其他系统设施（如 vMotion）不一定非要使用此 VLAN。
多个虚拟机是否共享同一个物理网络?	是	将这些虚拟机配置在同一个物理网络中。

表 15‑7 多客户开放部署中的组件共享（续）

功能	配置	备注
是否共享网络适配器?	局部	通过为服务控制台配置专用虚拟交换机和虚拟网络适配器来对其进行隔离。虚拟机或其他系统设施不一定非要使用此交换机或适配器。 但是，可以将所有虚拟机配置在同一个虚拟交换机和网络适配器上。
是否共享 VMFS?	是	虚拟机可以共享 VMFS 分区，并且其虚拟机 .vmdk 文件可以驻留在共享分区上。虚拟机不共享 .vmdk 文件。
安全级别	高	根据需要打开 FTP 等服务的端口。
虚拟机内存是否过量使用?	是	为虚拟机配置的总内存多于总物理内存。

表 15‑8 显示了设置主机用户帐户的方式。

表 15‑8 多客户开放部署中的用户帐户设置

用户类别	帐户总数
站点管理员	1
客户管理员	10
系统管理员	0
商业用户	0

表 15‑9 显示了每个用户的访问级别。

表 15‑9 多客户开放部署中的用户访问

访问级别	站点管理员	客户管理员	系统管理员	商业用户
是否具有根用户访问权限?	是	否	否	否
是否通过 SSH 进行服务控制台访问?	是	是	否	否
vCenter Server 和 vSphere Web Access?	是	是	否	否
是否创建和修改虚拟机?	是	是	否	否
是否通过控制台进行虚拟机访问?	是	是	是	是

虚拟机建议

在评估虚拟机安全性和管理虚拟机时，请考虑以下几个安全预防措施。

安装防病毒软件

由于每台虚拟机都承载着标准操作系统，因此应考虑安装防病毒软件，使其免遭病毒感染。根据虚拟机的使用方式，可能还需要安装软件防火墙。

请错开病毒扫描的调度，尤其是在具有大量虚拟机的部署中。如果同时扫描所有虚拟机，环境中的系统性能将大幅下降。

因为软件防火墙和防病毒软件需要占用大量虚拟化资源，因此您可以根据虚拟机性能平衡这两个安全措施的需求，尤其是在您确信虚拟机处于充分可信的环境中时。

限制公开复制到剪贴板中的敏感数据

默认情况下，已禁用针对 ESX 的复制和粘贴操作，以防止公开已复制到剪贴板中的敏感数据。

当在运行 VMware Tools 的虚拟机上启用复制和粘贴时，可以在客户机操作系统和远程控制台之间进行复制和粘贴。控制台窗口获得焦点时，虚拟机中运行的非特权用户和进程均可以访问虚拟机控制台的剪贴板。如果用户在使用控制台前将敏感信息复制到剪贴板中，就可能在无意中向虚拟机暴露敏感数据。为防止此问题，默认情况下已禁用针对客户机操作系统的复制和粘贴操作。

可以在必要时为虚拟机启用复制和粘贴操作。

启用客户机操作系统和远程控制台之间的复制和粘贴操作

要在客户机操作系统和远程控制台之间进行复制和粘贴，必须使用 vSphere Client 启用复制和粘贴操作。

步骤

1 使用 vSphere Client 登录到 vCenter Server 系统并选择虚拟机。

2 在**摘要**选项卡中，单击**编辑设置**。

3 选择**选项 > 高级 > 常规**，然后单击**配置参数**。

4 单击**添加行**，并在“名称”和“值”列中键入以下值。

名称	值
isolation.tools.copy.disable	false
isolation.tools.paste.disable	false

注意 这些选项将替代在客户机操作系统的 VMware Tools 控制面板中做出的任何设置。

5 单击**确定**以关闭“配置参数”对话框，然后再次单击**确定**以关闭“虚拟机属性”对话框。

6 重新启动虚拟机。

移除不必要的硬件设备

虚拟机上不具有特权的用户和进程可以连接或断开硬件设备（如网络适配器和 CD-ROM 驱动器）。因此，移除不需要的硬件设备有助于阻止攻击。

攻击者可利用该能力以多种方式破坏虚拟机的安全。例如，具有虚拟机访问权限的攻击者可以连接已断开的 CD-ROM 驱动器并访问遗留在驱动器中介质上的敏感信息，或者断开网络适配器以将虚拟机与其网络隔离，从而造成拒绝服务。

作为常规安全预防措施，可以使用 vSphere Client **配置**选项卡上的命令移除所有不需要或无用的硬件设备。虽然此举可提高虚拟机的安全性，但对于需要稍后恢复当前未使用的设备以提供服务的情况来说，这并非是一个好的解决方案。

阻止虚拟机用户或进程与设备断开连接

如果不想永久移除设备，可以阻止虚拟机用户或进程在客户机操作系统中连接设备或与设备断开连接。

步骤

1 使用 vSphere Client 登录到 vCenter Server 系统。

2 在“清单”面板中选择虚拟机。

3 在**摘要**选项卡中，单击**编辑设置**。

4 选择**选项 > 常规选项**，并记录下**虚拟机配置文件**文本框中显示的路径。

5 登录服务控制台并获取 root 特权。

6 更改目录以访问虚拟机配置文件（在步骤 4 中记录了其路径）。

   虚拟机配置文件位于 `/vmfs/volumes/datastore` 目录中，其中，*datastore* 是虚拟机文件驻留的存储设备的名称。例如，如果从“虚拟机属性”对话框获取的虚拟机配置文件为 `[vol1]vm-finance/vm-finance.vmx`，请更改为以下目录。

   ```
   /vmfs/volumes/vol1/vm-finance/
   ```

7 使用文本编辑器将以下行添加到 `.vmx` 文件，其中，*device_name* 是要保护的设备的名称（例如，`ethernet1`）。

   ```
   device_name.allowGuestConnectionControl = "false"
   ```

   注意 默认情况下，以太网 0 配置为不允许断开设备连接。除非以前的管理员将 `device_name.allowGuestConnectionControl` 设置为 `true`，否则无需更改该设置。

   ---

8 保存更改并关闭文件。

9 在 vSphere Client 中，右键单击虚拟机，并选择**关闭**。

10 右键单击虚拟机并选择**启动**。

限制客户机操作系统写入主机内存

客户机操作系统进程会通过 VMware Tools 向 ESX 主机发送信息性消息。如果不限制主机存储这些消息的数据量，则无限的数据流将为攻击者提供发起拒绝服务 (DoS) 攻击的机会。

客户机操作进程发送的信息性消息称之为 `setinfo` 消息，并且通常包含定义虚拟机特性的名称/值对或主机存储的标识符，例如，`ipaddress=10.17.87.224`。包含这些名称/值对的配置文件大小限制为 1 MB，这样可防止攻击者通过编写模仿 VMware Tools 的软件并使用任意配置数据填写主机内存，从而占用虚拟机所需的空间来发动 DoS 攻击。

如果名称/值对需要超过 1 MB 的存储空间，则可以根据需要更改值。另外，还可以阻止客户机操作系统进程将任何名称/值对写入到配置文件。

修改客户机操作系统的可变内存限制

如果配置文件中存储的自定义信息较多，可以增加客户机操作系统的可变内存限制。

步骤

1 使用 vSphere Client 登录到 vCenter Server 系统。

2 在“清单”面板中选择虚拟机。

3 在**摘要**选项卡中，单击**编辑设置**。

4 选择**选项** > **高级** > **常规**，然后单击**配置参数**。

5 如果不存在大小限制属性，则必须添加它。

   a 单击**添加行**。

   b 在“名称”列中，键入 **`tools.setInfo.sizeLimit`**。

   c 在“值”列中，键入 **`Number of Bytes`**。

   如果大小限制属性存在，请修改该属性以反映相应的限制。

6 单击**确定**以关闭“配置参数”对话框，然后再次单击**确定**以关闭“虚拟机属性”对话框。

阻止客户机操作系统进程向主机发送配置消息

可以阻止客户机将任何名称/值对写入到配置文件中。该选择适合必须阻止客户机操作系统修改配置设置的情况。

步骤

1 使用 vSphere Client 登录到 vCenter Server 系统。

2 在“清单”面板中选择虚拟机。

3 在**摘要**选项卡中，单击**编辑设置**。

4 选择**选项 > 高级 > 常规**，然后单击**配置参数**。

5 单击**添加行**，并在“名称”和“值”列中键入以下值。

   - 在“名称”列中：**isolation.tools.setinfo.disable**
   - 在“值”列中：**true**

6 单击**确定**以关闭“配置参数”对话框，然后再次单击**确定**以关闭“虚拟机属性”对话框。

配置客户机操作系统的日志记录级别

虚拟机可以将故障排除信息写入存储在 VMFS 卷上的虚拟机日志文件中。虚拟机用户和进程可能会有意或无意地误用日志记录，这会导致日志文件中充满大量数据。随着时间的推移，日志文件会占用大量文件系统空间，从而造成拒绝服务。

为避免该问题，可考虑修改虚拟机客户机操作系统的日志记录设置。这些设置可以限制日志文件的总大小和数量。通常，在每次重新引导主机时都会生成一个新的日志文件，因此文件会变的非常大。通过限制日志文件的最大大小，可以确保更频繁的生成新日志文件。VMware 建议保存 10 个日志文件，每个文件的大小限制为 100 KB。这些值的大小足以让您捕获充分的信息，用以调试可能会出现的大多数问题。

每向日志写入一个条目，都会检查一遍日志的大小。如果超过了限制，下一个条目将写入新的日志。如果存在的日志文件数量达到最大，则会删除最早的日志文件。通过写入超大的日志条目可以尝试发动避免这些限制的 DoS 攻击，但由于每个日志条目的大小限制在 4 KB 以下，因此，日志文件的大小不会比配置限制大 4 KB 以上。

限制日志文件数目和大小

要阻止虚拟机用户和进程淹没日志文件（可能造成服务拒绝），可以限制 ESX 生成的日志文件的数量和大小。

步骤

1 使用 vSphere Client 登录到 vCenter Server 系统。

2 在**摘要**选项卡中，单击**编辑设置**。

3 选择**选项 > 常规选项**，并记录下**虚拟机配置文件**文本框中显示的路径。

4 登录服务控制台并获取根特权。

5 更改目录以访问虚拟机配置文件（在步骤 3 中记录了其路径）。

   虚拟机配置文件位于 `/vmfs/volumes/`*`datastore`* 目录中，其中，*datastore* 是虚拟机文件驻留的存储设备的名称。例如，如果从“虚拟机属性”对话框获取的虚拟机配置文件为 `[vol1]vm-finance/vm-finance.vmx`，请更改为以下目录。

   `/vmfs/volumes/vol1/vm-finance/`

6 要限制日志大小，请使用文本编辑器添加以下行到 `.vmx` 文件并对其进行编辑，其中，*maximum_size* 是最大文件大小（单位是字节）。

   `log.rotateSize=`*`maximum_size`*

   例如，要将大小限制为 100 KB 左右，请输入 **100000**。

7 要保留有限数量的日志文件，请使用文本编辑器添加以下行到 `.vmx` 文件并对其进行编辑，其中，*number_of_files_to_keep* 是服务器保留的文件数。

```
log.keepOld=number_of_files_to_keep
```

例如，要保留 10 个日志文件（达到 10 个文件后，在创建新文件时删除最早的文件），请输入 **10**。

8 保存更改并关闭文件。

禁用客户机操作系统的日志记录

如果选择不将故障排除信息写入 VMFS 卷上存储的虚拟机日志文件，则可以同时停止日志记录。

如果禁用客户机操作系统的日志记录，请注意您可能无法收集到充足的日志以进行故障排除。而且，如果在禁用日志后出现虚拟机问题，VMware 不提供技术支持。

步骤

1 使用 vSphere Client 登录 vCenter Server，然后在清单中选择虚拟机。

2 在**摘要**选项卡中，单击**编辑设置**。

3 单击**选项**选项卡，并在“高级”下方的选项列表中选择**常规**。

4 在“设置”中，取消选中**启用日志记录**。

5 单击**确定**，关闭“虚拟机属性”对话框。

主机配置文件

管理主机配置文件 16

主机配置文件功能可用于创建配置文件，该配置文件会封装并帮助管理主机配置，尤其是在管理员管理 vCenter Server 中多个主机或群集的环境中。

主机配置文件通过使用主机配置文件策略，来消除每个主机的主机配置、手动主机配置或基于 UI 的主机配置，并维持数据中心内的配置一致性和正确性。这些策略捕获已知且经验证的引用主机的配置蓝图，并将其用于在多个主机或群集上配置网络、存储、安全和其他设置。然后，可以对照配置文件的配置检查主机或群集有无任何偏差。

本章讨论了以下主题：

主机配置文件使用情况模型

本主题描述使用主机配置文件的工作流程。

必须安装了 vSphere 而且至少有一台正确配置的主机。

1 设置并配置将作为引用主机使用的主机。

   引用主机是从中创建配置文件的主机。

2 使用指定的引用主机创建配置文件。

3 使用配置文件连接主机或群集。

4 对照配置文件检查主机的合规性。这样可以确保主机得以继续正确配置。

5 将引用主机的主机配置文件应用到其他主机或主机群集。

注意 只有 VMware vSphere 4.0 主机支持主机配置文件。VI 3.5 或更低版本的主机不支持此功能。如果拥有由 vCenter Server 4.0 管理的 VI 3.5 或更低版本的主机，那么，在您尝试使用这些主机的主机配置文件时，可能会出现以下情况：

- 无法创建使用 VMware Infrastructure 3.5 或更低版本主机作为引用主机的主机配置文件。
- 无法将主机配置文件应用到任何 VI 3.5 或更低版本主机。合规性检查失败。
- 在可以将主机配置文件连接到包含 VI 3.5 或更低版本主机的混合群集时，这些主机的合规性检查失败。

作为 vSphere 的一项许可功能，主机配置文件仅在获得相应的许可时才可用。如果发现错误，请确保具有针对所拥有主机的相应 vSphere 授权许可。

如果希望主机配置文件使用目录服务进行身份验证，则需要配置引用主机以使用目录服务。有关说明，请参见第 162 页，“配置主机以使用目录服务”。

访问主机配置文件视图

“主机配置文件”主视图列出所有可用的配置文件。管理员还可以使用“主机配置文件”主视图在主机配置文件上执行操作，并配置这些配置文件。

“主机配置文件”主视图应当由希望执行主机配置文件操作并配置高级选项和策略的有经验的管理员使用。大多数操作，诸如创建新配置文件、附加实体和应用配置文件等，都可以在“主机和群集”视图中执行。

步骤

◆ 选择**视图 > 管理 > 主机配置文件**。

所有的现有配置文件都将在配置文件列表左侧列出。从配置文件列表中选择配置文件时，该配置文件的详细信息将在右侧显示。

创建主机配置文件

通过使用指定引用主机的配置，可创建新的主机配置文件。

可以从以下位置创建主机配置文件：

- “主机配置文件”主视图
- 主机的上下文菜单

从主机配置文件视图创建主机配置文件

通过使用现有主机的配置，可以从“主机配置文件”主视图创建主机配置文件。

前提条件

必须存在 vSphere 安装，并且清单中至少有一台正确配置的主机。

步骤

1 在“主机配置文件”主视图中，单击**创建配置文件**。

   此时会出现创建配置文件向导。

2 选择与创建新配置文件相对应的选项，然后单击**下一步**。

3 选择要用于创建配置文件的主机，然后单击**下一步**。

4 键入名称，输入新配置文件的描述，然后单击**下一步**。

5 检查新配置文件的摘要信息，然后单击**完成**以完成配置文件的创建。

新配置文件将出现在配置文件列表中。

从主机创建主机配置文件

可以从“主机和群集”清单视图中的主机的上下文菜单中创建新的主机配置文件。

前提条件

必须存在 vSphere 安装，并且清单中至少有一台正确配置的主机。

步骤

1 在“主机和群集”视图中，选择要指定为新主机配置文件的引用主机的主机。

2 右键单击主机，然后选择**主机配置文件 > 从主机创建配置文件**

即会打开从主机创建配置文件向导。

3 键入名称，输入新配置文件的描述，然后单击**下一步**。

4 检查新配置文件的摘要信息，然后单击**完成**以完成配置文件的创建。

新配置文件即出现在主机的“摘要”选项卡中。

导出主机配置文件

可以将配置文件导出到 VMware 配置文件格式 (`.vpf`) 的文件中。

注意 导出主机配置文件时，将不导出管理员密码。此操作是一个安全措施，防止管理员密码在配置文件导出时以纯文本导出。配置文件导入后，系统将提示您重新输入密码值，该密码将应用于主机。

步骤

1 在“主机配置文件”视图页面中，从配置文件列表中选择要导出的配置文件。

2 右键单击配置文件，然后选择**导出配置文件**。

3 选择位置，并键入要将配置文件导出到的文件名称。

4 单击**保存**。

导入主机配置文件

可以从 VMware 配置文件格式 (`.vpf`) 的文件中导入配置文件。

注意 导出主机配置文件时，将不导出管理员密码。此操作是一个安全措施，防止管理员密码在配置文件导出时以纯文本导出。配置文件导入后，系统将提示您重新输入密码值，该密码将应用于主机。

步骤

1 在“主机配置文件”主视图中，单击**创建配置文件**图标。

此时会出现创建配置文件向导。

2 选择与导入配置文件相对应的选项，然后单击**下一步**。

3 输入或浏览要导入的 VMware 配置文件格式文件，然后单击**下一步**。

4 键入名称，输入已导入配置文件的描述，完成后单击**下一步**。

5 检查已导入配置文件的摘要信息，然后单击**完成**以完成配置文件的导入。

已导入的配置文件将出现在配置文件列表中。

编辑主机配置文件

可以查看和编辑主机配置文件策略，选择要进行合规性检查的策略，并更改策略名称或描述。

步骤

1 在“主机配置文件”主视图中，从配置文件列表中选择要编辑的配置文件。

2 单击**编辑主机配置文件**。

3 （可选）在配置文件编辑器顶部的字段中更改配置文件名称或描述。

4 编辑策略。

5 （可选）启用或禁用策略合规性检查。

6 单击**确定**，关闭配置文件编辑器。

编辑策略

策略描述应当如何应用特定的配置设置。使用配置文件编辑器，可以编辑属于特定主机配置文件的策略。

在配置文件编辑器的左侧，可以展开主机配置文件。每个主机配置文件由多个子配置文件组成，这些子配置文件由功能组指定，用以表示配置实例。每个子配置文件包含多个策略和合规性检查，这些策略和检查描述与配置文件相关的配置。

每个策略由一个或多个选项组成，这些选项中包括一个或多个参数。参数包括密钥和值。值的基本类型可以是以下几种：整数、字符串、字符串数组或整数数组。

可以配置的子配置文件（以及示例策略和合规性检查）包括：

表 16–1 主机配置文件的子配置文件配置

子配置文件配置	示例策略和合规性检查
内存预留	将内存预留设置为固定值。
存储器	配置 NFS 存储器。
网络	配置虚拟交换机、端口组、物理网卡速度、安全和网卡绑定策略、vNetwork 分布式交换机和 vNetwork 分布式交换机上行链路端口。
日期和时间	配置服务器的时间设置和时区。
防火墙	启用或禁用规则集。
安全	添加用户或用户组，设置根密码。
服务	配置服务的设置。
高级	修改高级选项。

步骤

1 打开要编辑的配置文件的配置文件编辑器。

2 在配置文件编辑器的左侧，展开子配置文件，直到进入要编辑的策略。

3 选择该策略。

在配置文件编辑器的右侧，策略选项和参数显示在“配置详细信息”选项卡中。

4 从下拉菜单中选择策略选项，并设置其参数。

5 （可选）如果对策略进行了更改，但希望恢复到默认选项，请单击**恢复**，选项即会重置。

启用合规性检查

可以决定是否对主机配置文件策略进行合规性检查。

步骤

1 打开某个配置文件的配置文件编辑器，导航到要启用合规检查的策略。

2 在配置文件编辑器的右侧，选择**合规性详细信息**选项卡。

3 启用与该策略相对应的复选框。

注意 如果禁用该复选框，则不会对该策略进行合规性检查，但仍会对启用了合规性检查的其他策略进行检查。

管理配置文件

创建主机配置文件之后，便可通过将配置文件附加到特定主机或群集来管理配置文件，然后将该配置文件应用到主机或群集。

连接实体

需要配置的主机会连接到配置文件。

配置文件还可以附加到群集。为确保合规性，所连接群集内的所有主机都必须按照相应的配置文件进行配置。当将主机添加到群集时，主机不会根据群集附加的主机配置文件自动进行配置。当将主机添加到已附加配置文件的群集时，主机会自动附加该配置文件。如果配置文件未应用，或未配置给配置文件中所指定的项，这将会导致下次执行合规性检查时配置文件的合规性状态呈现为失败。可通过将配置文件应用到主机来解决该问题。

可以从以下位置将主机或群集连接到配置文件：

- “主机配置文件”主视图
- 主机的上下文菜单
- 群集的上下文菜单
- 群集的“配置文件合规性”选项卡

从主机配置文件视图连接实体

在将配置文件应用到实体（主机或主机的群集）之前，需要将实体连接到配置文件。

可以从“主机配置文件”主视图将主机或群集连接到配置文件。

步骤

1 在“主机配置文件”主视图中，从配置文件列表中选择要为其添加附件的配置文件。

2 单击**连接主机/群集**图标。

3 从展开的列表中选择主机或群集，然后单击**附加**。

此时主机或群集将添加到“已附加实体”列表。

4 （可选）单击**分离**，从主机或群集中移除附件。

5 单击**确定**关闭该对话框。

从主机连接实体

在将配置文件应用到主机之前，需要将主机连接到配置文件。

可以从“主机和群集”清单视图中的主机上下文菜单中将配置文件连接到主机。

步骤

1 在“主机和群集”视图中，选择要将配置文件连接到的主机。

2 右键单击该主机，然后选择**主机配置文件 > 管理配置文件**。

注意 如果清单中不存在任何主机配置文件，则会出现一个对话框，询问您是否要创建配置文件并将主机连接到该配置文件。

3 在“附加配置文件”对话框中，选择要连接到主机的配置文件，然后单击**确定**。

即会在主机的**摘要**选项卡中更新主机配置文件。

应用配置文件

要将主机置于配置文件中指定的所需状况，请将配置文件应用到主机。

可以从以下位置将配置文件应用到主机：

- “主机配置文件”主视图
- 主机的上下文菜单
- 群集的“配置文件合规性”选项卡

从主机配置文件视图应用配置文件

可以从“主机配置文件”主视图将配置文件应用到主机。

前提条件

将配置文件应用到主机之前，该主机必须处于维护模式。

步骤

1 在“主机配置文件”主视图中，选择要应用到主机的配置文件。

2 选择**主机和群集**选项卡。

所连接的主机的列表显示在“实体名称”下。

3 单击**应用配置文件**。

在配置文件编辑器中，系统可能会提示您输入应用配置文件所需的参数。

4 输入参数，然后单击**下一步**。

5 继续操作，直到输入完所需的全部参数。

6 单击**完成**。

合规性状态即会进行更新。

从主机应用配置文件

可以从主机的上下文菜单中将配置文件应用到主机。

前提条件

将主机应用到配置文件之前，该主机必须处于维护模式

步骤

1 在“主机和群集”视图中，选择要向其应用配置文件的主机。

2 右键单击主机，然后选择**主机配置文件 > 应用配置文件**。

3 在配置文件编辑器中，输入参数，然后单击**下一步**。

4 继续操作，直到输入完所需的全部参数。

5 单击**完成**。

合规性状态即会进行更新。

更改引用主机

引用主机配置用于创建主机配置文件。

可以从“主机配置文件”主视图或从主机的上下文菜单中执行此任务。

前提条件

主机配置文件必须已经存在。

步骤

1 可以从“主机配置文件”主视图或从主机中执行此任务。

   - 在“主机配置文件”主视图中，右键单击要更改其引用主机的配置文件，然后选择**更改引用的主机**。
   - 在“主机和群集”视图中，右键单击要更新其引用的主机，然后选择**管理配置文件**。

   即会打开“分离或更改主机配置文件”对话框。

2 确定是要从主机或群集分离配置文件，还是更改配置文件的引用主机。

   - 单击**分离**可移除主机和配置文件之间的关联。
   - 单击**更改**可继续更新配置文件的引用主机。

   如果选择的是**更改**，则将打开“附加配置文件”对话框。配置文件引用的当前主机将显示为**引用主机**。

3 展开清单列表，并选择要将配置文件连接到的主机。

4 单击**更新**。

   即会更新**引用主机**。

5 单击**确定**。

主机配置文件的“摘要”选项卡将列出更新的引用主机。

从群集管理配置文件

可以从群集的上下文菜单创建配置文件、连接配置文件或更新引用主机。

步骤

◆ 在“主机和群集”视图中，右键单击群集，然后选择**主机配置文件 > 管理配置文件**。根据您的主机配置文件设置，将出现以下结果之一：

配置文件状态和任务	结果
如果群集未连接到主机配置文件且清单中不存在任何配置文件，请创建一个配置文件。	a 将打开一个对话框，询问是否要创建配置文件并将其连接到群集。 b 如果选择**是**，则将打开“创建配置文件”向导。
如果群集未连接到主机配置文件且清单中存在一个或多个配置文件，请连接一个配置文件。	a 将打开“附加配置文件”对话框。 b 选择要连接到群集的配置文件，然后单击**确定**。
如果群集已连接到一个主机配置文件，则可分离该配置文件或连接到另一个配置文件。	在此对话框中，单击**分离**从群集中分离配置文件，或单击**更改**将其他配置文件连接到群集。

从引用主机更新配置文件

如果从其创建配置文件的主机（引用主机）的配置发生变化，可以更新配置文件，以便其配置与引用主机的配置相匹配。

创建主机配置文件之后，可能需要对配置文件进行增量更新。可以使用两种方法执行此任务：

- 在 vSphere Client 中对引用主机进行配置更改，然后从引用主机更新配置文件。现有配置文件中的设置将被更新，以匹配引用主机的设置。
- 可使用配置文件编辑器直接更新配置文件。

虽然从配置文件编辑器更新配置文件可能更全面，且提供了更多选项，但从引用主机更新配置文件，您可以先验证配置，然后再将其传输到附加该配置文件的其他主机。

从引用主机更新配置文件在“主机配置文件”主视图中执行。

步骤

◆ 在“主机配置文件”主视图中，右键单击要更新的配置文件，然后选择**从引用主机更新配置文件**。

检查合规性

检查合规性可确保主机或群集得以继续正确配置。

在为主机或群集配置了引用主机配置文件之后，可能会发生手动更改，导致配置不正确。定期检查合规性可确保主机或群集得以继续正确配置。

从主机配置文件视图检查合规性

可以从“主机配置文件”主视图检查主机或群集是否符合配置文件。

步骤

1 从“主机配置文件”列表中，选择要检查的配置文件。

2 在**主机和群集**选项卡中，从“实体名称”下的列表中选择主机或群集。

3 单击**立即检查合规性**。

   合规性状态将更新为“合规”、“未知”或“不合规”。

   如果合规性状态是“不合规”，则可以将主机应用到配置文件。

从主机检查合规性

在将配置文件连接到主机之后，从主机的上下文菜单运行合规性检查以检验配置。

步骤

1 在“主机和群集”视图中，选择要在其上运行合规性检查的主机。

2 右键单击主机，然后选择**主机配置文件 > 检查合规性**。

   主机的合规性状态显示在主机的**摘要**选项卡中。

如果主机不合规，则必须将配置文件应用到该主机。

检查群集合规性

可以对照主机配置文件或特定的群集要求和设置来检查群集合规性。

步骤

1 在“主机和群集”视图中，选择要在其上运行合规性检查的群集。

2 在“配置文件合规性”选项卡中，单击**立即检查合规性**，将针对连接到此群集的主机配置文件和群集要求（如果有）检查群集的合规性。

   - 系统会检查群集是否符合群集内主机的特定设置（如 DRS、HA 和 DPM）。例如，它可能检查是否启用了 vMotion。群集要求的合规性状态将进行更新。即使主机配置文件未连接到群集，也会执行此检查。
   - 如果主机配置文件已连接到群集，则将检查群集是否符合主机配置文件。主机配置文件的合规性状态将进行更新。

3 （可选）单击“群集要求”旁边的**描述**可获得特定群集要求的列表。

4 （可选）单击“主机配置文件”旁边的**描述**可获得特定主机配置文件合规检查的列表。

5 （可选）单击**更改**可更改连接到群集的主机配置文件。

6 （可选）单击**移除**可分离连接到群集的主机配置文件。

如果群集与配置文件不符，则必须将配置文件分别应用到群集内的每台主机。

附录

ESX 技术支持命令



此附录中的大多数命令专供技术支持使用并仅供参考。但在少数情况下，这些命令也提供为主机执行配置任务的唯一方式。此外，如果丢失了与主机的连接，则通过命令行界面执行这些命令中的某一命令可能是您唯一可以求助的方式 — 例如，如果网络不起作用，vSphere Client 也因此不可用。

注意 如果使用此附录中的命令，则必须执行 `service mgmt-vmware restart` 命令重新启动 `vmware-hostd` 进程，同时警示 vSphere Client 及其他管理工具，通知其配置已更改。通常情况下，如果主机当前正由 vSphere Client 或 vCenter Server 管理，则不要执行本附录中的命令。

vSphere Client 图形用户界面提供了执行本主题中所述配置任务的首选方式。可以使用本主题来判断应使用哪个 vSphere Client 命令来代替这些命令。本主题提供在 vSphere Client 中执行的操作摘要，但并未给出完整的说明。有关使用命令和通过 vSphere Client 执行配置任务的详细信息，请参见联机帮助。

登录服务控制台并使用 `man <esxcfg_command_name>` 命令显示手册页，可找到有关多个 ESX 命令的其他信息。

表 A-1 列出了为 ESX 提供的技术支持命令，概述了每个命令的用途并说明了对应的 vSphere Client 命令。只有在您从“清单”面板中选择了 ESX 主机并单击**配置**选项卡之后，才可以执行该表中列出的大多数 vSphere Client 操作。除非另有声明，否则这些操作即为下述任一过程的预备步骤。

表 A-1 ESX 技术支持命令

命令	命令用途和 vSphere Client 过程
`esxcfg-advcfg`	配置 ESX 的高级选项。 要在 vSphere Client 中配置高级选项，请单击**高级设置**。“高级设置”对话框打开时，使用左侧的列表选择要使用的设备类型或活动，然后输入适当的设置。
`esxcfg-auth`	配置身份验证。可使用此命令在 `pam_cracklib.so` 和 `pam_passwdqc.so` 插件之间切换，以便实施密码更改规则。也可使用此命令来重置这两个插件的选项。 在 vSphere Client 中无法配置这些功能。
`esxcfg-boot`	配置引导程序设置。此命令适用于引导程序进程，并仅供 VMware 技术支持使用。除非得到 VMware 技术支持代表指示，否则不得发出此命令。 在 vSphere Client 中无法配置这些功能。
`esxcfg-dumppart`	配置诊断分区或搜索现有诊断分区。 在安装 ESX 时，将自动创建诊断分区，用于在发生系统故障时存储调试信息。除非确定主机没有诊断分区，否则无需手动创建此分区。 可在 vSphere Client 中对诊断分区执行以下管理操作： ■ 确定是否有诊断分区 — 单击**存储器** > **添加存储器**，然后检查**添加存储器**向导的第一个页面以查看其是否包括**诊断**选项。如果没有**诊断**选项，则 ESX 已具有一个诊断分区。 ■ 配置诊断分区 — 单击**存储器** > **添加存储器** > **诊断**，然后一步步完成向导。

表 A–1 ESX 技术支持命令（续）

命令	命令用途和 vSphere Client 过程
`esxcfg-firewall`	配置服务控制台防火墙端口。 要在 vSphere Client 中为支持的服务和代理配置防火墙端口，请选择将允许其访问 ESX 主机的 Internet 服务。单击**安全配置文件 > 防火墙 > 属性**，然后使用**防火墙属性**对话框添加服务。 通过 vSphere Client 无法配置不受支持的服务。对于这些服务，请使用 `esxcfg-firewall`。
`esxcfg-info`	打印有关服务控制台、VMkernel、虚拟网络中各种子系统以及存储资源硬件的状况信息。 vSphere Client 不提供打印此信息的方法，但可以通过用户界面中的不同选项卡和功能获得尽可能多的信息。例如，通过检查**虚拟机**选项卡上的信息，可以查看虚拟机的状态。
`esxcfg-init`	执行内部初始化例程。此命令适用于引导程序进程，不得在任何情况下使用此命令。使用此命令可能导致 ESX 主机出现问题。 此命令不存在 vSphere Client 等效指令。
`esxcfg-module`	设置驱动程序参数和修改在启动时加载的驱动程序。此命令适用于引导程序进程，并仅供 VMware 技术支持使用。除非得到 VMware 技术支持代表指示，否则不得发出此命令。 此命令不存在 vSphere Client 等效指令。
`esxcfg-mpath`	为光纤通道或 iSCSI 磁盘配置多路径设置。 要在 vSphere Client 中为存储器配置多路径设置，请单击**存储器**。选择数据存储或映射的 LUN，然后单击**属性**。**属性**对话框打开时，根据需要选择所需的数据区。然后单击**数据区设备 > 管理路径**，然后使用**管理路径**对话框配置路径。
`esxcfg-nas`	管理 NFS 挂载。使用此命令创建或卸载 NFS 数据存储。 要在 vSphere Client 中查看 NFS 数据存储，请单击**存储器 > 数据存储**，然后滚动查看数据存储列表。也可以从**存储器 > 数据存储**视图执行以下活动： ■ 显示 NFS 数据存储的属性 – 单击数据存储并检查**详细信息**下的信息。 ■ 创建 NFS 数据存储 – 单击**添加存储器**。 ■ 卸载 NFS 数据存储 – 单击**移除**，或右键单击要卸载的数据存储并选择**卸载**。
`esxcfg-nics`	打印物理网络适配器的列表以及有关驱动程序、PCI 设备和每个网卡的链接状况的信息。也可使用此命令来控制物理网络适配器的速度和双工模式。 要查看有关 vSphere Client 中主机的物理网络适配器的信息，请单击**网络适配器**。 要更改 vSphere Client 中物理网络适配器的速度和双工模式，请单击与物理网络适配器相关联的任意虚拟交换机的**网络 > 属性**。在**属性**对话框中，单击**网络适配器 > 编辑**，然后选择速度和双工组合。
`esxcfg-resgrp`	恢复资源组设置并允许您执行基本资源组管理。 从”清单“面板中选择一个资源池，然后单击**摘要**选项卡上的**编辑设置**以更改资源组设置。
`esxcfg-route`	设置或检索默认 VMkernel 网关路由，并添加、移除或列出静态路由。 要在 vSphere Client 中查看默认的 VMkernel 网关路由，请单击 **DNS 和路由**。要更改默认的路由，请单击**属性**，然后更新 **DNS 和路由配置**对话框中这两个选项卡的信息。
`esxcfg-swiscsi`	配置软件 iSCSI 软件适配器。 要在 vSphere Client 中配置软件 iSCSI 系统，请单击**存储适配器**，选择要配置的 iSCSI 适配器，然后单击**属性**。使用 **iSCSI 启动器属性**对话框配置适配器。

表 A–1 ESX 技术支持命令 （续）

命令	命令用途和 vSphere Client 过程
`esxcfg-upgrade`	从 ESX Server 2.x 升级到 ESX。此命令不适用于一般用途。 从 2.x 升级到 3.x 时完成以下三个任务。以下任务可在 vSphere Client 中执行： ■ 升级主机 — 升级二进制数据，从 ESX Server 2.x 转换成 ESX。不能从 vSphere Client 中执行此步骤。 ■ 升级文件系统 — 要将 VMFS-2 升级到 VMFS-3，请挂起或关闭虚拟机，然后单击**清单 > 主机 > 进入维护模式**。单击**存储器**，选择存储设备，然后单击**升级到 VMFS-3**。必须为要升级的每个存储设备执行此步骤。 ■ 升级虚拟机 — 要将虚拟机从 VMS-2 升级到 VMS-3，请右键单击”清单“面板中的虚拟机，然后选择**升级虚拟机**。
`esxcfg-scsidevs`	打印 VMkernel 存储设备至服务控制台设备的映射。此命令不存在 vSphere Client 等效指令。
`esxcfg-vmknic`	创建和更新 vMotion、NAS 和 iSCSI 的 VMkernel TCP/IP 设置。 要在 vSphere Client 中设置 vMotion、NFS 或 iSCSI 网络连接，请单击**网络 > 添加网络**。选择 **VMkernel**，然后一步步完成**添加网络向导**。在**连接设置**步骤中定义 IP 地址子网掩码和 VMkernel 默认网关。 要查看设置，请单击 vMotion、iSCSI 或 NFS 端口左侧的蓝色图标。要编辑任何这些设置，请单击交换机的**属性**。从交换机**属性**对话框上的列表中选择端口，然后单击**编辑**以打开端口**属性**对话框，然后更改端口的设置。
`esxcfg-vswif`	创建和更新服务控制台网络设置。如果因网络配置问题无法通过 vSphere Client 管理 ESX 主机，则使用此命令。 要在 vSphere Client 中设置服务控制台连接，请单击**网络 > 添加网络**。选择**服务控制台**，然后一步步完成“添加网络向导”。在**连接设置**步骤中定义 IP 地址子网掩码和服务控制台默认网关。 要查看设置，请单击服务控制台端口左侧的蓝色图标。要编辑任何这些设置，请单击交换机的**属性**。从交换机**属性**对话框上的列表中选择服务控制台端口。单击**编辑**以打开端口**属性**对话框，然后更改端口设置。
`esxcfg-vswitch`	创建和更新虚拟机网络设置。 要在 vSphere Client 中设置虚拟机连接，请单击**网络 > 添加网络**。选择**虚拟机**，然后一步步完成**添加网络向导**。 要查看设置，请单击虚拟机端口组左侧的语言泡状图标。要编辑任何这些设置，请单击交换机的**属性**。从交换机**属性**对话框上的列表中选择虚拟机端口，然后单击**编辑**以打开端口**属性**对话框，然后更改端口的设置。

用于 ESX 的 Linux 命令

B

为了支持特定的内部操作，ESX 安装包括标准 Linux 配置命令的子集，例如网络和存储器配置命令。使用这些命令执行配置命令可能导致严重的配置冲突并造成部分 ESX 功能不可用。

除非 vSphere 文档中另有说明或者得到 VMware 技术支持人员指示，否则在配置 ESX 时始终通过 vSphere Client 工作。

使用 vmkfstools C

可以使用 vmkfstools 实用程序来创建和操作 VMware ESX 主机上的虚拟磁盘、文件系统、逻辑卷和物理存储设备。

使用 vmkfstools 可以在磁盘的物理分区上创建和管理虚拟机文件系统 (VMFS)。还可以使用此命令操作文件，例如存储在 VMFS-2、VMFS-3 和 NFS 上的虚拟磁盘文件。

可使用 vSphere Client 执行大多数 vmkfstools 操作。

本附录讨论了以下主题：

vmkfstools 命令语法

一般而言，不需要以 root 用户身份登录来运行 vmkfstools 命令。但是，某些命令（例如文件系统命令），可能需要以 root 用户身份登录。

下面是与 vmkfstools 命令配合使用的参数：

- *options* 为一个或多个命令行选项及相关联的参数，用于指定 vmkfstools 要执行的活动， 例如，在创建新虚拟磁盘时选择磁盘格式。

  输入选项以后，通过输入 /vmfs 层次结构中的相对或绝对文件路径名，指定要在其中执行操作的文件或 VMFS 文件系统。

- *partition* 指定文件分区。此参数采用 vml.*vml_ID*:P 格式，其中 *vml_ID* 是由存储阵列返回的设备 ID，而 P 是表示分区号的整数。分区数字必须大于零 (0)，并对应于类型为 fb 的有效 VMFS 分区。

- *device* 指定设备或逻辑卷。此参数使用 ESX 设备文件系统中的路径名。路径名以 /vmfs/devices 开头，这是设备文件系统的挂载点。

  指定不同类型的设备时，具体格式如下：

  - /vmfs/devices/disks 适用于本地磁盘或基于 SAN 的磁盘。
  - /vmfs/devices/lvm 适用于 ESX 逻辑卷。
  - /vmfs/devices/generic 适用于通用 SCSI 设备，例如磁带驱动器。

- *path* 指定 VMFS 文件系统或文件。此参数是对目录符号链接、裸设备映射或 /vmfs 下的文件进行命名的绝对或相对路径。

  - 要指定 VMFS 文件系统，请使用以下格式：

    /vmfs/volumes/*file_system_UUID*

或

`/vmfs/volumes/file_system_label`

- 要指定 VMFS 文件，请使用以下格式：

  `/vmfs/volumes/file system label|file system UUID/[dir]/myDisk.vmdk`

  如果当前的工作目录是 myDisk.vmdk 的父目录，则不必输入完整路径。

  例如，

  `/vmfs/volumes/datastore1/rh9.vmdk`

vmkfstools 选项

vmkfstools 命令有多个选项。其中的一些选项仅建议高级用户使用。

长格式和单字母格式的选项表示相同含义。例如，下面的命令是一样的。

```
vmkfstools --createfs vmfs3 --blocksize 2m vml.vml_ID:1
vmkfstools -C vmfs3 -b 2m vml.vml_ID:1
```

-v 子选项

-v 子选项表示命令输出的详细级别。

该子选项的格式如下：

```
-v --verbose number
```

可以指定 *number* 的值，范围是从 1 到 10 的整数。

使用任何 vmkfstools 选项都可以指定 -v 子选项。如果选项的输出不适合于 -v 子选项，则 vmkfstools 将忽略 -v。

注意 由于可以将 -v 子选项包含在任何 vmkfstools 命令行中，因此 -v 不作为子选项纳入选项描述中。

文件系统选项

文件系统选项可用于创建 VMFS 文件系统。这些选项不适用于 NFS。这些任务中有许多是可以通过 vSphere Client 执行的。

创建 VMFS 文件系统

使用 vmkfstools 命令可以创建 VMFS 文件系统。

```
-C --createfs vmfs3
-b --blocksize block_sizekK|mM
-S --setfsname fsName
```

本选项将在指定的 SCSI 分区（例如 vml.*vml_ID*:1）上创建 VMFS-3 文件系统。该分区将成为文件系统的主分区。

在任何 ESX 主机上，VMFS-2 文件系统都是只读的。您不能创建或修改 VMFS-2 文件系统，但可以读取 VMFS-2 文件系统上存储的文件。VMFS-3 文件系统不能从 ESX 2.x 主机进行访问。



小心 一个 LUN 只能有一个 VMFS 卷。

可以与 -C 选项一同指定以下子选项：

- -b --blocksize – 定义 VMFS-3 文件系统的块大小。默认的块大小为 1 MB。指定的 *block_size* 值必须是 128 KB 的倍数，最小值为 128 KB。输入大小值时，请加上后缀 m 或 M 以表明单位类型。单位类型不区分大小写。vmkfstools 会将 m 或 M 的含义理解为兆字节，将 k 或 K 的含义理解为千字节。
- -S --setfsname - 为正在创建的 VMFS-3 文件系统定义 VMFS 卷的卷标。此子选项只与 -C 选项结合使用。指定的卷标最多为 128 个字符，并且在开头和结尾不能包含空格。

  在定义卷标之后，则可以在为 vmkfstools 命令指定 VMFS 卷时使用此卷标。卷标将显示在为 Linux ls -l 命令生成的列表中，并且作为指向 /vmfs/volumes 目录下 VMFS 卷的符号链接。

  要更改 VMFS 卷标，请使用 Linux ln -sf 命令。可参考以下示例：

  ```
  ln -sf /vmfs/volumes/UUID /vmfs/volumes/fsName
  ```

  fsName 是用于 *UUID* VMFS 的新卷标。

创建 VMFS 文件系统的示例

此示例说明如何在 vml.*vml_ID*:1 分区上创建名为 my_vmfs 的新 VMFS-3 文件系统。文件块大小为 1 MB。

```
vmkfstools -C vmfs3 -b 1m -S my_vmfs /vmfs/devices/disks/vml.vml_ID:1
```

扩展现有的 VMFS-3 卷

使用 vmkfstools 命令可以将数据区添加到 VMFS 卷。

```
-Z --extendfs extention-device existing-VMFS-volume
```

此选项将为以前创建的 VMFS 卷 *existing-VMFS-volume* 添加另一个数据区。必须指定完整路径名称（例如 /vmfs/devices/disks/vml.*vml_ID*:1），而不只是短名称（例如 vml.*vml_ID*:1）。每次使用此选项时，都会使用新数据区扩展 VMFS-3 卷，因此该卷将跨多个分区。逻辑 VMFS-3 卷最多可以包含 32 个物理数据区。



小心 运行此选项时，之前在 *extension-device* 中指定的 SCSI 设备上保存的所有数据均将丢失。

扩展 VMFS-3 卷的示例

此示例允许逻辑文件系统跨到新分区，以对其进行扩展。

```
vmkfstools -Z /vmfs/devices/disks/vml.vml_ID_2:1
/vmfs/devices/disks/vml.vml_ID_1:1
```

扩展后的文件系统跨越两个分区 - vml.*vml_ID_1*:1 和 vml.*vml_ID_2*:2。在此示例中，vml.*vml_ID_1*:1 是主分区的名称。

列出 VMFS 卷的属性

使用 vmkfstools 命令可以列出 VMFS 卷的属性。

```
-P --queryfs
-h --human-readable
```

当此选项用于任何驻留在 VMFS 卷上的文件或目录时，它将列出指定卷的属性。列出的属性包括 VMFS 版本号（VMFS-2 或 VMFS-3）、包含指定的 VMFS 卷的数据区个数、卷标（如果有）、UUID 以及各个数据区所驻留的设备名称列表。

注意 如果任何设备的后备 VMFS 文件系统脱机，则数据区的数量以及可用的空间也将相应更改。

可以在使用 -P 选项时指定 -h 子选项。如果这样，则 vmkfstools 将以可读性更强的形式（例如，5k、12.1M 或 2.1G）列出卷容量。

将 VMFS-2 升级到 VMFS-3

可以将 VMFS-2 文件系统升级到 VMFS-3。



小心 VMFS-2 至 VMFS-3 的转换是一种单向过程。将 VMFS-2 卷转换成 VMFS-3 后，就不能再转换回 VMFS-2 卷。

仅当 VMFS-2 文件系统的文件块大小未超过 8 MB 时，才可对其进行升级。

升级文件系统时，请使用以下选项：

- `-T --tovmfs3 -x --upgradetype [zeroedthick|eagerzeroedthick|thin]`

  该选项将 VMFS-2 文件系统转换成 VMFS-3，同时保留文件系统中的所有文件。转换之前，请使用模块选项 `fsauxFunction=upgrade` 卸载 `vmfs2` 和 `vmfs3` 驱动程序并加载辅助文件系统驱动程序 `fsaux`。

  必须使用 `-x --upgradetype` 子选项将升级类型指定为以下任一种：

  - `-x zeroedthick`（默认）- 保留 VMFS-2 厚文件的属性。通过 `zeroedthick` 文件格式，磁盘空间将分配至文件以备将来使用，并且未使用的数据块也不会置零。
  - `-x eagerzeroedthick` – 转换时将厚文件中的未使用数据块置零。如果使用此子选项，则升级过程会比使用其他选项要长得多。
  - `-x thin` – 将 VMFS-2 厚文件转换成精简置备的 VMFS-3 文件。与 `thick` 文件格式相反，精简置备的格式不允许为文件分配额外空间以备将来使用，它采用的是按需使用空间。转换时将放弃 `thick` 文件中未使用的块。

  在转换期间，ESX 文件锁定机制将确保没有其他本地进程访问正在转换的 VMFS 卷，同时也必须确保没有远程的 ESX 主机正在访问此卷。转换可能需时几分钟，完成后将返回到命令提示符。

  转换后，卸载 `fsaux` 驱动程序并加载 `vmfs3` 和 `vmfs2` 驱动程序以继续正常操作。

- `-u --upgradefinish`

  此选项可完成升级。

虚拟磁盘选项

虚拟磁盘选项可用于设置、迁移和管理存储在 VMFS-2、VMFS-3 和 NFS 文件系统中的虚拟磁盘。其中的大部分任务也可以通过 vSphere Client 执行。

受支持的磁盘格式

创建或克隆虚拟磁盘时，可以使用 `-d --diskformat` 子选项来指定磁盘格式。

从以下格式中选择：

- `zeroedthick`（默认）- 创建时为虚拟磁盘分配所需空间。创建时不会擦除物理设备上保留的任何数据，但是以后从虚拟机首次执行写操作时会按需要将其置零。虚拟机不从磁盘读取失效数据。
- `eagerzeroedthick` - 创建时为虚拟磁盘分配所需空间。与 `zeroedthick` 格式相比，在创建时会将物理设备上保留的数据置零。创建这种格式的磁盘所需的时间可能会比创建其他类型的磁盘长。
- `thick` - 创建时为虚拟磁盘分配所需空间。这种类型的格式化不会将可能存在于该分配空间中的任何旧数据置零。非 root 用户不允许创建此格式。
- `thin` - 精简置备的虚拟磁盘。与 `thick` 格式不同，它在创建时不会为虚拟磁盘分配所需的空间，只会在将来需要时再提供或置零。
- `rdm` - 虚拟兼容模式裸磁盘映射。
- `rdmp` - 物理兼容模式（直通）裸磁盘映射。

- raw - 裸设备。
- 2gbsparse - 最大数据区为 2 GB 的稀疏磁盘。可将此格式的磁盘用于其他 VMware 产品，但是，除非先使用 vmkfstools 以兼容的格式（例如 thick 或 thin）重新导入磁盘，否则无法在 ESX 主机上启动稀疏磁盘。
- monosparse – 单片式稀疏磁盘。可将此格式的磁盘用于其他 VMware 产品。
- monoflat – 单片式平面磁盘。可将此格式的磁盘用于其他 VMware 产品。

注意 对于 NFS 只能使用 thin、thick、zerodthick 和 2gbsparse 等磁盘格式。

thick、zeroedthick 和 thin 通常具有相同的意义，因为决定分配策略的是 NFS 服务器而非 ESX 主机。大多数 NFS 服务器上的默认分配策略是 thin。

创建虚拟磁盘

使用 vmkfstools 命令可以创建虚拟磁盘。

```
-c --createvirtualdisk size[kK|mM|gG]
-a --adaptertype [buslogic|lsilogic] srcfile
-d --diskformat [thin|zeroedthick|eagerzeroedthick]
```

此选项将在 VMFS 卷上的指定路径创建虚拟磁盘。指定虚拟磁盘的大小。为 *size* 输入值时，可以加上 k（千字节）、m（兆字节）或 g（千兆字节）等后缀以指明其单位类型。单位类型不区分大小写。vmkfstools 会将 k 或 K 的含义理解为千字节。如果不指定单位类型，vmkfstools 将默认为字节。

可以与 -c 选项一同指定以下子选项。

- -a 指定用于与虚拟磁盘进行通信的设备驱动程序。可以在 BusLogic 和 LSI Logic SCSI 这两个驱动程序间选择。
- -d 指定磁盘格式。

创建虚拟磁盘的示例

此示例说明如何在名为 myVMFS 的 VMFS 文件系统中创建一个名为 rh6.2.vmdk、大小为 2 GB 的虚拟磁盘文件。此文件表示一个可由虚拟机访问的空虚拟磁盘。

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/rh6.2.vmdk
```

初始化虚拟磁盘

使用 vmkfstools 命令可以初始化虚拟磁盘。

```
-w --writezeros
```

此选项通过在虚拟磁盘的所有数据上写入零数据以将其清空。完成此命令的时间可能较长，具体取决于虚拟磁盘的大小以及承载虚拟磁盘的设备的 I/O 带宽。



小心 使用此命令时将丢失虚拟磁盘上的所有现有数据。

填充精简虚拟磁盘

使用 vmkfstools 命令可以填充精简虚拟磁盘。

```
-j --inflatedisk
```

此选项将 thin 虚拟磁盘转换成 eagerzeroedthick，并保留所有现有数据。此选项对尚未分配的任何块进行分配和置零。

移除置零的块

使用 `vmkfstools` 命令可将任何精简、zeroedthick 或 eagerzeroedthick 虚拟磁盘转换成移除了置零块的精简磁盘。

```
-K --punchzero
```

此选项解除分配所有置零的块，并仅保留那些以前分配的且包含有效数据的块。得到的虚拟磁盘为精简格式。

将 Zeroedthick 虚拟磁盘转换成 Eagerzeroedthick 磁盘

使用 `vmkfstools` 命令可将任何 zeroedthick 虚拟磁盘转换成 eagerzeroedthick 磁盘。

```
-k --eagerzero
```

在执行该转换时，此选项会保留虚拟磁盘上的任何数据。

删除虚拟磁盘

此选项将删除与 VMFS 卷上指定路径中列出的虚拟磁盘相关联的文件。

```
-U --deletevirtualdisk
```

重命名虚拟磁盘

此选项将重命名与在命令行的路径规范部分中列出的虚拟磁盘相关联的文件。

您必须指定原始文件名或文件路径 *oldName*，以及新文件名或文件路径 *newName*。

```
-E --renamevirtualdisk oldName newName
```

克隆虚拟磁盘或裸磁盘

此选项将创建指定虚拟磁盘或裸磁盘的副本。

```
-I --importfile srcfile -d --diskformat
[rdm:device|rdmp:device|
raw:device|thin|2gbsparse|monosparse|monoflat]
```

您可使用 `-I` 选项的 `-d` 子选项。此子选项将为所创建的副本指定磁盘格式。不允许非 root 用户克隆虚拟磁盘或裸磁盘。

注意 要克隆 ESX Redo 日志，同时保留其层次结构，请使用 `cp` 命令。

克隆虚拟磁盘的示例

此示例说明如何将主虚拟磁盘的内容从 `templates` 存储库克隆到 `myVMFS` 文件系统上名为 `myOS.vmdk` 的虚拟磁盘文件中。

```
vmkfstools -I /vmfs/volumes/templates/gold-master.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
```

可以通过将配置行添加到虚拟机配置文件来将虚拟机配置为使用此虚拟磁盘，如下例所示：

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

迁移 VMware Workstation 和 VMware GSX Server 虚拟机

不能使用 vSphere Client 将通过 VMware Workstation 或 VMware GSX Server 创建的虚拟机迁移到 ESX 系统中。但是，可以使用 `vmkfstools -I` 命令将虚拟磁盘导入 ESX 系统，然后将此磁盘附加到在 ESX 中创建的新虚拟机上。

必须先导入虚拟磁盘，因为不能在 ESX 主机上启动以 `2gbsparse` 格式导出的磁盘。

步骤

1 将 Workstation 或 GSX Server 磁盘导入 `/vmfs/volumes/myVMFS/` 目录或任何子目录。

2 在 vSphere Client 中，使用**自定义**配置选项创建新虚拟机。

3 配置磁盘时，选择**使用现有虚拟磁盘**并连接已导入的 Workstation 或 GSX Server 磁盘。

扩展虚拟磁盘

此选项可在创建虚拟机后，对分配至虚拟机的磁盘大小进行扩展。

`-X --extendvirtualdisk` *`newSize`*`[kK|mM|gG]`

输入此命令之前，必须先关闭使用此磁盘文件的虚拟机。必须更新磁盘上的文件系统，以便客户机操作系统能够识别和使用新的磁盘大小，并利用额外的空间。

通过分别添加 `k`（千字节）、`m`（兆字节）或 `g`（千兆字节）等后缀，可以将 `newSize` 参数指定为千字节、兆字节或千兆字节。单位类型不区分大小写。`vmkfstools` 会将 `k` 或 `K` 的含义理解为千字节。如果不指定单位类型，`vmkfstools` 将默认为千字节。

上述 `newSize` 参数将重新定义整个磁盘的大小，而不是定义给磁盘增加的大小。

例如，要给 4 G 的虚拟磁盘增加 1 G，则输入：**`vmkfstools -X 5g`** ***`disk name`*** **`.dsk`**

注意 请勿对具有相关快照的虚拟机的基础磁盘进行扩展。否则，您再也不能提交快照或将基础磁盘转换回原始大小。

将 VMFS-2 虚拟磁盘迁移至 VMFS-3

此选项可以将指定的虚拟磁盘文件从 ESX Server 2 格式转换成 ESX 格式。

`-M --migratevirtualdisk`

创建虚拟兼容性模式裸设备映射

此选项将在 VMFS-3 卷上创建裸设备映射 (RDM) 文件，并将裸磁盘映射至该文件。在建立映射后，便可以像访问普通 VMFS 虚拟磁盘那样访问裸磁盘。映射文件的长度与其所指向的裸磁盘的大小相同。

`-r --createrdm` *`device`*

当指定 *device* 参数时，具体格式如下：

`/vmfs/devices/disks/vml.`*`vml_ID`*

注意 所有的 VMFS-3 文件锁定机制均适用于 RDM。

创建虚拟兼容模式 RDM 的示例

在此示例中，创建名为 `my_rdm.vmdk` 的 RDM 文件，并将 `vml.`*`vml_ID`* 裸磁盘映射到该文件。

`vmkfstools -r /vmfs/devices/disks/vml.`*`vml_ID`*` my_rdm.vmdk`

通过将下行添加到虚拟机配置文件中，可以将虚拟机配置为使用 `my_rdm.vmdk` 映射文件：

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

创建物理兼容模式裸设备映射

通过此选项，可以将直通裸设备映射到 VMFS 卷上的文件。该映射使虚拟机在访问其虚拟磁盘时能够规避 ESX SCSI 命令的筛选。当虚拟机需要发送专用的 SCSI 命令时，例如当 SAN 感知软件在虚拟机中运行时，此类映射将非常有用。

`-z --createrdmpassthru` *`device`*

在建立了此类映射后，便可以使用该映射像访问任何其他 VMFS 虚拟磁盘那样访问裸磁盘了。

当指定 *device* 参数时，具体格式如下：

`/vmfs/devices/disks/vml.`*`vml_ID`*

列出 RDM 的属性

此选项可列出裸磁盘映射的属性。

`-q --queryrdm`

此选项将列出裸磁盘 RDM 的名称。此选项还列出裸磁盘的其他标识信息，例如磁盘 ID。

显示虚拟磁盘几何形状

此选项可获得有关虚拟磁盘几何形状的信息。

`-g --geometry`

输出内容的形式如下：`Geometry information C/H/S`，其中 `C` 代表磁道的数量，`H` 代表磁头的数量，而 `S` 代表扇区的数量。

注意 在将 VMware Workstation 虚拟磁盘导入 ESX 主机时，可能会看到磁盘几何形状不匹配的错误消息。磁盘几何形状不匹配也可能是因为加载客户机操作系统或运行新创建的虚拟机时出现了问题。

检查和修复虚拟磁盘

使用此选项可在出现非正常关机时检查或修复虚拟磁盘。

`-x , -fix [check|repair]`

管理 LUN 的 SCSI 预留

`-L` 选项可用于为物理存储设备执行管理任务。其中的大部分任务可以通过 vSphere Client 执行。

`-L --lock [reserve|release|lunreset|targetreset|busreset]`*`device`*

通过该选项，可以预留 SCSI LUN（使其供 ESX 主机专用）、解除预留（使其他主机可以访问 LUN）和重置预留（以强制从目标解除所有预留）。



小心 使用 `-L` 选项可以中断 SAN 中其他服务器的操作。仅在排除群集设置故障时使用 `-L` 选项。

除非得到 VMware 的特别通知，否则决不要针对承载 VMFS 卷的 LUN 使用此选项。

可以通过几种方式指定 `-L` 选项：

- `-L reserve` – 预留指定的 LUN。预留指定的 LUN 后，只有预留该 LUN 的服务器才能访问它。如果其他服务器尝试访问该 LUN，将导致预留错误。
- `-L release` – 解除对于指定 LUN 的预留。其他服务器可再次访问该 LUN。
- `-L lunreset` – 重置指定的 LUN，方法是清除 LUN 上的所有预留，并使 LUN 再次对所有服务器可用。重置对设备上的其他 LUN 没有影响。在设备上预留的其他 LUN 仍保持预留状态。

- `-L targetreset` – 重置整个目标。重置将清除与该目标关联的所有 LUN 上的各个预留，并使 LUN 再次对所有服务器可用。
- `-L busreset` – 重置总线上所有可访问的目标。重置将清除可通过总线访问的所有 LUN 上的任何预留，并使其再次对所有服务器可用。

当输入 *device* 参数时，具体格式如下：

/vmfs/devices/disks/vml.*vml_ID*:P

索引